



str.Alexandru cel Bun nr.13, MD-2003, oraşul Durleşti, municipiul Chişinău, Republica Moldova, tel.+373 22 58-44-78,
fax: +373 22 58-44-78, e-mail: durlestiprimarie@gmail.com

Nr. 62-d din 16 iunie 2021

DISPOZIȚIE

**Cu privire la implementarea prevederilor
Politicii de Securitate privind protecția datelor cu
caracter personal la prelucrarea acestora
în cadrul sistemelor informaționale
gestionate de Primăria or. Durleşti**

În scopul asigurării securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal în procesul de activitate a Primăriei or. Durleşti, întru respectarea prevederilor Hotărârii Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal, Hotărârii Guvernului nr. 296/2012 privind aprobarea Regulamentului Registrului de evidență a operatorilor de date cu caracter personal, în temeiul articolului 29 alineatul (2) din Legea nr. 436/2006 privind administrația publică locală,

DISPUN :

1. Se aprobă Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă, conform anexei nr. 1.
 - 1.1. Se desemnează titularul funcției de contabil șef adjunct al Primăriei or. Durleşti, persoană reponsabilă pentru protecția datelor cu caracter personal din sistemul de evidență contabilă.
2. Se aprobă Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență al resurselor umane din cadrul Primăriei or. Durleşti, conform anexei nr. 2.
 - 2.1. Se desemnează titularul funcției de secretar al Consiliului or. Durleşti, persoană reponsabilă pentru protecția datelor cu caracter personal din sistemul de evidență al resurselor umane.
3. Se aprobă Regulamentul Registrului de evidență a corespondenței al Primăriei or. Durleşti, conform anexei nr. 3.
4. Se aprobă Regulamentul Registrului de evidență al petițiilor parvenite în adresa Administrației Publice Locale a or. Durleşti, conform anexei nr. 4.
5. Controlul asupra executării prevederilor prezentei mi-l asum.
6. Prezenta Dispoziție poate fi contestată la Judecătoria Chişinău, sediul Râşcani, str. Kiev 3, mun. Chişinău, în termen de 30 de zile de la data publicării.

Primar



Eleonora ȘARAN



Anexa nr. 1

Aprobat
prin Dispoziția Primarului or. Durlești
nr. 62 din 16 iunie 2021



REGULAMENTUL PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ

I. DISPOZIȚII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă (în continuare Regulament) este elaborat în vederea implementării în cadrul Administrației Publice Locale or. Durlești (în continuare – APL Durlești), a prevederilor Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Legii contabilității nr. 113 din 27 aprilie 2007 (Se aplica față de autoritățile/instituțiile bugetare), Legii contabilității și raportării financiare nr. 287 din 15 decembrie 2017 și a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, precum și întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților APL Durlești în cadrul sistemului de evidență contabilă.

II. SCOPUL

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă constă în asigurarea înregistrării informațiilor contabile referitoare la calculul drepturilor salariale ale angajaților, inclusiv a premiilor, stimulărilor, sporurilor, indemnizațiilor, compensațiilor și altor drepturi și obligații cu conținut pecuniar, precum și a prezentării rapoartelor financiare, trimestriale și anuale către instituțiile statului, conform legislației în vigoare.

2.2. În cadrul sistemului de evidență contabilă sînt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele și patronimicul;
- numărul personal de identificare de stat (IDNP);
- data nașterii și domiciliul;
- codul personal de asigurări sociale (CPAS);
- codul personal de asigurări medicale (CPAM);
- 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 obligatorii de asistență medicală și socială, și alte sume datorate în virtutea legii sau contractului;
- după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.

2.3. Prelucrarea datelor cu caracter personal menționate va fi efectuată pentru realizarea următoarelor scopuri:

- a) Prelucrarea informației privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajații APL Durlești și care au impact asupra calculării plăților salariale, precum și a persoanelor fizice și juridice cu care APL Durlești intră în relații contractuale;
- b) Calcularea drepturilor salariale lunare, în conformitate cu legislația în vigoare a Republicii Moldova (conform contractelor individuale de muncă, contractelor civile, tabelor de pontaj, ordinelor/dispozițiilor conducerii, raportului de activitate lunară);
- c) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor de incapacitate temporară de muncă;
- d) Prelucrarea copiilor ordinelor/dispozițiilor conducerii referitoare la personal;
- e) Calcularea și reținerea taxelor ce țin de plățile salariale aferente angajaților: primele de asigurare obligatorie de asistență medicală, contribuțiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.;
- f) 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;
- g) Furnizarea informației necesare pentru elaborarea rapoartelor lunare privind contribuțiile de asigurare socială de stat obligatorii (forma IPC18) și rapoartelor trimestriale privind primele de asigurare obligatorie de asistență medicală (forma IRM19);
- h) Întocmirea, lunară, a declarației persoanei asigurate REV 5 pentru fiecare angajat și transmiterea acestora Casei Teritoriale de Asigurări Sociale, în format electronic prin SIA E-REPORTING cu aplicarea semnăturii digitale;
- i) Asistarea procesului (prin furnizarea informației necesare) pentru completarea periodică (lunară) a raportului și dării de seamă privind venitul achitat și impozitul pe venit reținut din acesta;
- j) Completarea lunară, trimestrială și anuală a dărilor de seamă cu prezentarea acestora Inspectoratului Fiscal de Stat, precum și perfectarea și eliberarea informației privind veniturile calculate și achitate în folosul persoanei fizice și impozitul pe venit reținut din aceste venituri angajaților APL Durlești.
- k) 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;
- l) Eliberarea certificatelor de salariu, la cererea angajaților;
- m) Completarea și stocarea fișelor personale de evidență a veniturilor sub formă de salariu și alte plăți efectuate de către patron în folosul angajatului pe fiecare an, precum și a impozitului pe venit reținut din aceste plăți (Anexa nr. 8 la Ordinul IFPS nr.676 din 14.12.2007);
- n) Emiterea, transmiterea și primirea documentelor financiar-contabile (facturi, anexe la facturi, documente justificative, acte de prestare servicii);
- o) Prezentarea documentelor financiare ce conțin date cu caracter personal către acționari/fondatori, comisiei de cenzori, auditului intern sau extern.



2.4. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt 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 rămîne la păstrare primind statut de document de arhivă.

2.5. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență contabilă în alte scopuri decît cele menționate mai sus este interzisă.

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ CONTABILĂ

3.1. Datele cu caracter personal conținute în sistemul de evidență contabilă în cadrul APL Durlești se prelucrează/stocheză:

1. pe suport de hîrtie;
 2. în format electronic:
- a) Software – Sistemul de evidență contabilă IC Entreprise, versiunea 3.188.210408 care este instalat la computerul central – „Contabil Șef” și cu drept de acces la al doilea computer – „Materiale”, computerele aflîndu-se în biroul 16 din sediul APL Durlești, str. Așexandru cel Bun nr. 13, or. Durlești ;
 - b) Hardware – calculator nr de inventariere 31460445

3.2. Mentenanța programului contabil IC Entreprise este efectuată de către compania VVS SOFTWARE SRL, fiind încheiat anual contract de valoare mică privind prestarea serviciilor de deservire între APL Durlești și compania VVS SOFTWARE SRL __, cu următoarele atribuții stabilite companiei prestatoare:

- Efectuarea ajustărilor în program, în baza modificărilor legislației Republicii Moldova;
- Eliminarea erorilor în funcționarea programului;
- Consultarea în rezolvarea dificultăților apărute în utilizarea programului (Linia fierbinte);
- Examinarea solicitărilor parvenite din partea _____;
- Examinarea bazei de date a _____ (la necesitate);
- Vizite la fața locului, la solicitarea _____;
- Examinarea și nedivulgarea informației cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

3.3. Prelucrarea informațiilor în sistemul de evidență contabilă pe suport de hîrtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sînt amplasate fizic în biroul/birourile 16 din sediul APL Durlești, str. Așexandru cel Bun nr. 13, or. Durlești.

IV. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidență contabilă se efectuează pe perioada valabilității contractelor de achiziție publică, pe perioada activității angajaților sediul APL Durlești, str. Așexandru cel Bun nr. 13, or. Durlești (din momentul semnării contractului pînă la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

4.2. La expirarea termenelor menționate în punctul 4.1., datele din sistemul de evidență contabilă sînt păstrate în formă arhivată, pe perioada stabilită de --- **Nomenclatorul dosarelor din cadrul APL Durlești.**



V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. APL Durlești, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.

5.2. 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.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență contabilă vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii APL Durlești. Informațiile furnizate vor fi acordate astfel, încât 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.

5.5. 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.

5.6. Prelucrarea datelor cu caracter personal în sistemul de evidență contabilă se efectuează în conformitate cu prevederilor art. 5 alin. 5 lit. a), b) și e) al Legii privind protecția datelor cu caracter personal.

VI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ

6.1. Măsurile generale de administrare a securității informaționale

6.1.1. În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronic care conțin date preluate din sistemul de evidență contabilă, aceștia se păstrează în safeuri care se încuie.

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

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

6.1.4. Accesul fizic la mijloacele de reprezentare a informației preluate din sistemul de evidență contabilă este blocat împotriva vizualizării de către persoane neautorizate.

6.1.5. Mijloacele de prelucrare a informațiilor preluate din sistemul de evidență contabilă sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

6.1.6. Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență contabilă din/în perimetrul de securitate se înregistrează în registru.



6.2. Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul de evidență contabilă, se înfăptuiesc ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică.

6.3. Cerințe speciale față de marcarea: toate informațiile ieșite din sistemul de evidență contabilă, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului 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.

6.4. Accesul în biroul unde este amplasat sistemul de evidență contabilă 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.

6.5. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.

6.6. Înainte de acordarea accesului fizic la sistemul de evidență contabilă, se verifică competențele de acces.

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

6.8. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidență contabilă, fiind integru din punct de vedere fizic.

6.9. Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat sistemul de evidență contabilă, din punct de vedere fizic.

6.10. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.

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

6.12. Amplasarea sistemului de evidență contabilă răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

6.13. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului de evidență contabilă, 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 contabilă, inclusiv posibilitatea deconectării oricărui component TI.

6.14. Computerele, unde este amplasat fizic sistemul de evidență contabilă, dispun de UPS-uri, care sînt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

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



6.16. Securitatea antiincendiară a sistemului de evidență contabilă: biroul unde este amplasat sistemul de evidență contabilă este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiarie în vigoare.

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

VII. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENȚĂ CONTABILĂ

7.1. Este efectuată identificarea și autentificarea utilizatorilor informațiilor preluate din sistemele de evidență contabilă și a proceselor executate în numele acestor utilizatori.

7.2. 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.

7.3. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hîrtie, cu excepția cazului de asigurare a securității păstrării acestora (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

7.4. Se efectuează modificarea parolelor de fiecare dată cînd sînt depistați indicii unei eventuale compromiteri a sistemului sau parolei.

7.5. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sînt folosite identificatori și parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora. După trei tentative greșite de autentificare, accesul este blocat, în mod automatizat.

7.6. Se asigură, pentru o perioadă de 1 /un/ an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor și prevenirea folosirii repetate a acestora.

7.7. 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 3 luni), codurile de identificare și autentificare se revocă sau se suspendă.

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidență contabilă, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora. Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidență contabilă, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 /una/ lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informațiile din sistemul de evidență contabilă. Se folosesc



mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

7.9. 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 utilizatorilor la sistemul de evidență contabilă.

7.10. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autorizează de persoanele responsabile.

7.11. Se impun limite în privința persoanelor care au dreptul:

- a) să vizualizeze informațiile stocate în sistemul de evidență contabilă;
- b) să copieze, să descarce, să șteargă sau să modifice orice informație stocată.

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

7.13. Orice activitate de dezvăluire a datelor cu caracter personal către terți este documentată și supusă unei analize riguroase în prealabil privind scopul și temeiul legal a intențiilor de dezvăluire a unui anumit volum de date cu caracter personal.

7.14. Orice încălcare a securității în ceea ce privește sistemul de evidență contabilă este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

7.15. Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea sistemului de evidență contabilă este controlată și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

VIII. AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ CONTABILĂ

8.1. Se organizează generarea înregistrărilor de audit a securității în sistemul de evidență contabilă pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

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

- a) data și timpul tentativei intrării/ieșirii;
- b) ID-ul utilizatorului;
- c) rezultatul tentativei de intrare/ieșire – pozitivă sau negativă.

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din sistemele de evidență contabilă, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:

- a) data și timpul tentativei de pornire;
- b) denumirea/identificatorul programului aplicativ sau al procesului;
- c) ID-ul utilizatorului;
- d) rezultatul tentativei de pornire – pozitivă sau negativă.



8.4. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din sistemul de evidență contabilă, conform următorilor parametri:

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

8.5. Se efectuează înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

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

8.6. Se efectuează înregistrarea ieșirii din sistemul de evidență contabilă, înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:

- a) data și timpul eliberării;
- b) denumirea informației și căile de acces la aceasta;
- c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
- d) ID-ul utilizatorului care a solicitat informația;
- e) volumul documentului eliberat (numărul paginilor, fișelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.

8.7. Cazurile de deranjament al auditului securității în sistemul de evidență contabilă sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoștința persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

8.8. Rezultatele auditului securității în sistemul de evidență contabilă (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

8.9. Durata minimă a stocării rezultatelor auditului securității în sistemul de evidență contabilă constituie 2 /doi/ ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ CONTABILĂ

9.1. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din sistemul de evidență contabilă, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestora, 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.

9.2. Se utilizează tehnologii și mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor și constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informațiilor din sistemul de evidență contabilă.



9.3. Se asigură testarea funcționării corecte a componentelor de securitate a sistemului de evidență contabilă (automat – la pornirea sistemului, și după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

9.4. Copiile de siguranță: reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către operator intervalul de timp în care se execută copiile de siguranță a informațiilor din sistemul de evidență contabilă și soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ CONTABILĂ

10.1. Persoanele care asigură exploatarea sistemului de evidență contabilă trec, minimum o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență contabilă.

10.3. „În cazul producerii incidentelor de securitate persoanele responsabile va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar și să asigure accesul la informațiile necesare relevante obiectului controlului.”

10.4. Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din sistemul de evidență contabilă poartă răspundere civilă, contravențională și penală.

XI. DISPOZIȚII FINALE

11.1. Prezentul Regulament este revizuit și ulterior aprobat de către conducerea APL Durlești periodic, însă cel puțin o dată în an, precum și la necesitate.

11.2. Prezentul Regulament se completează cu prevederile legislației în vigoare.

11.3. Regulamentul este adus la cunoștința angajaților contra semnăturii.

11.4. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.



Anexa nr. 2

Aprobat

prin Dispoziția Primarului or. Durești nr. 62-ol

din 16 iulie 2021



REGULAMENTUL PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE

I. DISPOZIȚII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal (în continuare Regulament) este elaborat în vederea implementării în cadrul Autorității Publice Locale a or. Durești (în continuare- APL Durești) a prevederilor Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal și a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010, precum și întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților APL Durești în cadrul sistemului de evidență resurse umane (denumit în continuare "sistemul de evidență").

II. SCOPUL

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență constă în asigurarea înregistrării informațiilor referitoare la recrutarea, angajarea, executarea clauzelor contractelor individuale de muncă, pensionarea salariaților, precum și a prezentării rapoartelor trimestriale și anuale către instituțiile statului, conform legislației în vigoare.

2.2. În cadrul sistemului de evidență sunt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele, patronimicul;
- sexul;
- data și locul nașterii;
- semnătura;
- date din actele de stare civilă;
- CPAM;
- Telefon mobil;
- E-mail;
- Profesie, funcție;
- Formare profesională;
- Situația familială;
- Situație economică și financiară;
- Datele membrilor de familie;
- Cetățenia;
- Sancțiuni disciplinare;
- CPAS;
- Telefon/fax;
- Adresa (domiciliu/reședința);
- Loc de muncă;
- IDNP;



- Date bancare;
- Imagine:
- cetățenia;
- IDNP;
- imagine;
- mărime salariu brut, prime, stimulări, sporuri, suplimente, date din certificatul de concediu medical.
- după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.

2.3. Prelucrarea datelor cu caracter personal menționate în cadrul sistemului de evidență resurse umane va fi efectuată pentru realizarea următoarelor scopuri:

- a) Realizării activităților aferente recrutării;
- b) Încheierea și executarea contractelor de muncă;
- c) Furnizarea de beneficii;
- d) Prezentarea la CNAM a evidenței nominale a noilor angajați și a celor concediați, format hârtie și format electronic
- e) Administrarea resurselor umane la nivelul APL Durlești (de ex., evaluare, training, proceduri disciplinare, plata salariilor, registre de personal, asigurarea securității și sănătății în muncă);
- f) Desfășurarea de controale interne și externe de tip audit, cat si pentru cooperarea cu organizatiile profesionale;
- g) Arhivare, îndeplinirea obligațiilor legale, apărare în caz de litigiu sau orice formă de neînțelegere între salariat și APL Durlești.

2.4. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt 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 rămîne la păstrare primind statut de document de arhivă.

III. LOCAȚIA ȘI DESCRIEREA SISTEMUL DE EVIDENȚĂ RESURSE UMANE

3.1. Datele cu caracter personal conținute în sistemul de evidență în cadrul APL Durlești se prelucrează/stocheză pe suport de hîrtie.

3.2. Prelucrarea informațiilor în sistemul de evidență pe suport de hîrtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sînt amplasate fizic în biroul 7 din sediul or. Durlești strada Alexandru cel Bun nr. 13.

IV. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidență resurse umane se efectuează pe perioada activității angajaților APL Durlești, valabilității contractelor individuale de muncă (din momentul semnării contractului până la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

4.2. Datele cu caracter personal a potențialilor salariați se preia din CV-ul transmis de către aceștia la adresa de e-mail a APL Durlești. După primirea CV-ului prin intermediul poștei electronice, acesta se tipărește pe suport de hîrtie, iar de pe adresa de e-mail se șterge conținutul mesajului. Totodată, în cazul în care potențialii salariați nu au fost admiși la funcția vacantă din cadrul APL Durlești, atunci persoana responsabilă de sistemul de evidență a resurselor umane distruge CV-urile potențialilor angajați.

4.3. La expirarea termenelor menționate în punctul 4.1., datele din sistemul de evidență resurse umane sînt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul dosarelor APL Durlești aprobat prin Dispoziția Primarului or. Durlești sau Indicatorul documentelor-tip și al termenelor lor



de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Agenția Națională a Arhivelor nr.57 din 27.07.2016, ulterior fiind supuse distrugerii sau ștergerii, în funcție de suportul pe care au fost efectuate.

V. DREPTURILE PERSOANELOR VIZATE

- 5.1.** APL Durlești în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.
- 5.2.** 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.
- 5.3.** Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență vor respecta procedura de acces la datele cu caracter personal.
- 5.4.** Acordarea dreptului de acces a persoanelor vizate la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii APL Durlești. Informațiile furnizate vor fi acordate astfel, încât 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.
- 5.5.** 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.
- 5.6.** Prelucrarea datelor cu caracter personal ale potențialilor salariați, precum și a salariaților se efectuează în conformitate cu art. 5 alin. (5) lit. a) și lit. b) ale Legii privind protecția datelor cu caracter personal, și anume: în cazul executării unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înainte încheierii contractului, la cererea acestuia (în cazul încheierii contractului individual de muncă) și în cazul îndeplinirii unei obligații care îi revine operatorului conform legii (în conformitate cu legislația muncii).

VI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE

- 6.1.** Măsurile generale de administrare a securității informaționale.
- 6.1.1.** În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie care conțin date preluate din sistemul de evidență, aceștia se păstrează în safeuri care se încuie.
- 6.1.2.** La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.
- 6.1.3.** Operatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.
- 6.1.4.** Accesul fizic la mijloacele de reprezentare a informației preluate din sistemul de evidență este blocat împotriva vizualizării de către persoane neautorizate.
- 6.1.5.** Mijloacele de prelucrare a informațiilor preluate din sistemul de evidență sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
- 6.1.6.** Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență din/în perimetrul de securitate se înregistrează în registru.



6.2. Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul de evidență, se înfăptuiesc ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală.

6.3. Cerințe speciale față de marcarea: toate informațiile ieșite din sistemul de evidență, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului 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.

6.4. Accesul în birourile APL Durești este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program.

6.5. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior,.

6.6. Înainte de acordarea accesului fizic la sistemul de evidență, se verifică competențele de acces.

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

6.8. Perimetrul de securitate se consideră perimetrul birourilor în care este amplasat sistemul de evidență, fiind integre din punct de vedere fizic.

6.9. Zilnic, se inspectează perimetrele de securitate al clădirii și al biroului, din punct de vedere fizic.

6.10. Accesul persoanelor neautorizate în cadrul perimetrelor de securitate va fi chestionat pentru a evita accesul neautorizat și fiecare situație va fi raportată persoanelor responsabile cu acordarea drepturilor de acces și asigurarea securității.

6.11. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.

6.12. Amplasarea sistemului de evidență răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

6.13. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului de evidență, 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 sistemul de evidență, inclusiv posibilitatea deconectării oricărui component TI.

6.14. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor, sînt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiatul, cablurile de tensiune sînt separate de cele comunicaționale.

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



VII. AUDITUL SECURITĂȚII ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE

7.1. Se organizează generarea înregistrărilor de audit a securității în sistemul de evidență pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

7.2. Înregistrările de audit a securității sistemului de evidență în care sînt prelucrate date cu caracter personal, trebuie să conțină:

- numele și prenumele utilizatorului;
- numele fișei accesate (pagina și inscripția din registru);
- numărul înregistrărilor efectuate;
- tipul de acces;
- data accesului (an, lună, zi);
- timpul (ora, minuta) și durata accesului.

7.3. Rezultatele auditului securității în sistemul de evidență (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

7.4. Durata minimă a stocării rezultatelor auditului securității în sistemul de evidență constituie 2 /doi/ ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigațiile sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

VIII. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ RESURSE UMANE

8.1. Persoanele care asigură exploatarea sistemului de evidență trec, minimum o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

8.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență.

8.3. „În cazul producerii incidentelor de securitate persoanele responsabile vor întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar și să asigure accesul la informațiile necesare relevante obiectului controlului.”

8.4. Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din sistemul de evidență poartă răspundere civilă, contravențională și penală.

IX. Specificul legislației muncii privind prelucrarea datelor personale ale salariaților

9.1. În conformitate cu art. 91 al Codului Muncii, angajatorul și reprezentanții lui sunt obligați să respecte următoarele cerințe:

a) prelucrarea datelor personale ale salariatului poate fi efectuată exclusiv în scopul îndeplinirii prevederilor legislației în vigoare, acordării de asistență la angajare, instruirii și avansării în serviciu, asigurării securității personale a salariatului, controlului volumului și calității lucrului îndeplinit și asigurării integrității bunurilor unității;

- b) la determinarea volumului și conținutului datelor personale ale salariatului ce urmează a fi prelucrate, angajatorul este obligat să se conducă de legislația în vigoare;
- c) toate datele personale urmează a fi preluate de la salariat sau din sursa indicată de acesta;
- d) angajatorul nu este în drept să obțină și să prelucreze date referitoare la convingerile politice și religioase ale salariatului, precum și la viața privată a acestuia. În cazurile prevăzute de lege, angajatorul poate cere și prelucra date despre viața privată a salariatului numai cu acordul scris al acestuia;
- e) angajatorul nu este în drept să obțină și să prelucreze date privind apartenența salariatului la sindicate, asociații obștești și religioase, partide și alte organizații social-politice, cu excepția cazurilor prevăzute de lege;
- f) la adoptarea unei decizii care afectează interesele salariatului, angajatorul nu este în drept să se bazeze pe datele personale ale salariatului obținute exclusiv în urma prelucrării automatizate sau pe cale electronică;
- g) protecția datelor personale ale salariatului contra utilizării ilegale sau pierderii este asigurată din contul angajatorului;
- h) salariații și reprezentanții lor trebuie să fie familiarizați, sub semnătură, cu documentele vizând modul de prelucrare și păstrare a datelor personale ale salariaților din unitate și să fie informați despre drepturile și obligațiile lor în domeniul respectiv;
- i) salariații nu trebuie să renunțe la drepturile lor privind păstrarea și protecția datelor personale;
- j) angajatorii, salariații și reprezentanții lor trebuie să elaboreze în comun măsurile de protecție a datelor personale ale salariaților.

9.2. Conform art. 92 al CM, la transmiterea datelor personale ale salariatului, angajatorul trebuie să respecte următoarele cerințe:

- a) să nu comunice unor terți datele personale ale salariatului fără acordul scris al acestuia, cu excepția cazurilor când acest lucru este necesar în scopul prevenirii unui pericol pentru viața sau sănătatea salariatului, precum și a cazurilor prevăzute de lege;
- b) să nu comunice datele personale ale salariatului în scopuri comerciale fără acordul scris al acestuia;
- c) să prevină persoanele care primesc datele personale ale salariatului despre faptul că acestea pot fi utilizate doar în scopurile pentru care au fost comunicate și să ceară persoanelor în cauză confirmarea în scris a respectării acestei reguli. Persoanele care primesc datele personale ale salariatului sunt obligate să respecte regimul de confidențialitate, cu excepția cazurilor prevăzute de lege;
- d) să permită accesul la datele personale ale salariatului doar persoanelor împuternicite în acest sens, care, la rândul lor, au dreptul să solicite numai datele personale necesare exercitării unor atribuții concrete;
- e) să nu solicite informații privind starea sănătății salariatului, cu excepția datelor ce vizează capacitatea salariatului de a-și îndeplini obligațiile de muncă;
- f) să transmită reprezentanților salariaților datele personale ale salariatului în modul prevăzut de prezentul cod și să limiteze această informație numai la acele date personale care sunt necesare exercitării de către reprezentanții respectivi a atribuțiilor lor.

9.3. Conform art. 93 al CM, în scopul asigurării protecției datelor sale personale care se păstrează la angajator, salariatul are dreptul:

- a) de a primi informația deplină despre datele sale personale și modul de prelucrare a acestora;
- b) de a avea acces liber și gratuit la datele sale personale, inclusiv dreptul la copie de pe orice act juridic care conține datele sale personale, cu excepția cazurilor prevăzute de legislația în vigoare;
- c) de a-și desemna reprezentanții pentru protecția datelor sale personale;
- d) de a avea acces la informația cu caracter medical ce-l vizează, inclusiv prin intermediul lucrătorului medical, la alegerea sa;
- e) de a cere excluderea sau rectificarea datelor personale incorecte și/sau incomplete, precum și a datelor prelucrate cu încălcarea cerințelor prezentului cod. În cazul în care angajatorul refuză să excludă sau să rectifice datele personale incorecte, salariatul este în drept să notifice în scris angajatorului dezacordul său motivat;
- f) de a ataca în instanța de judecată orice acțiuni sau inacțiuni ilegale ale angajatorului admise la obținerea, păstrarea, prelucrarea și protecția datelor personale ale salariatului



X. DISPOZIȚII FINALE

10.1. Presentul Regulament este revizuit și ulterior aprobat de către conducerea APL Durlești periodic, însă cel puțin o dată în an, precum și la necesitate.

10.2. Presentul Regulament se completează cu prevederile legislației în vigoare.

10.3. Regulamentul este adus la cunoștința angajaților prin comunicare directă sau prin publicarea pe pagina de Internet a APL Durlești.

10.4. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.



Anexa nr. 3
Aprobat
Prin Dispoziția Primarului or. Durllești
nr. 64-d din 16 iunie 2021



REGULAMENTUL Registrului de evidență a corespondenței al Primăriei or. Durllești

I. Dispoziții generale

1. Regulamentul Registrului de evidență a corespondenței al Primăriei or. Durllești (Regulamentul) este elaborat în conformitate cu prevederile Codului administrativ al Republicii Moldova, aprobat prin Legea nr. 116 din 19 iulie 2018, Legii nr. 71-XVI din 22 martie 2007 cu privire la registre, Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Instrucțiunilor privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 208 din 31 martie 1995, Regulilor de întocmire a documentelor organizatorice și de dispoziție și Instrucțiunii-tip cu privire la ținerea lucrărilor de secretariat în organele administrației publice centrale de specialitate și ale autoadministrării locale ale Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 618 din 05 octombrie 1993, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010.

2. Prezentul Regulament reglementează modalitatea Ținerii Registrului de evidență a corespondenței Primăriei or. Durllești, precum și procedura de înregistrare, securizare, modificare și radiere a datelor din acest Registru.

3. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută de Legea cu privire la registre, Codului administrativ al Republicii Moldova, aprobat prin Legea nr. 116 din 19 iulie 2018, Legea privind protecția datelor cu caracter personal, Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

Astfel, în sensul prezentului Regulament se definesc următoarele noțiuni:

Petiție – orice cerere, sesizare sau propunere adresată unei autorități publice de către o persoană fizică sau juridică;

Cerere – orice cerere prin intermediul căreia se solicită emiterea unui act administrativ individual sau efectuarea unei operațiuni administrative;

Sesizare – orice sesizare prin intermediul căreia se informează autoritatea publică cu privire la o problemă de interes personal sau public;

Propunere – orice propune prin intermediul căreia se urmărește realizarea de către autoritatea publică a unor acțiuni de interes public;

Registrul de evidență a corespondenței – resursa informațională specializată (totalitatea informațiilor ținute în formă automatizată și manuală) care asigură evidența informației sistematizate, principalul obiectiv al căruia constă în asigurarea evidenței corespondenței parvenite la Primăria or. Durllești;

Registrator – angajatul Primăriei or. Durllești împuternicit cu atribuțiile de introducere, modificare, păstrare a informației din Registru.

Furnizorul datelor - persoana fizică sau reprezentantul persoanei juridice de drept public sau privat, care prezintă registratorului date despre obiectul registrului în modul stabilit de lege sau acord.

4. Subiecți ai raporturilor juridice apărute ca rezultat al instituirii, administrării și Ținerii manuale a Registrului sînt:

- Primăria or. Durllești, în calitate de proprietar și deținător al Registrului;
- Persoanele împuternicite de Ținerea Registrului și cele responsabile de efectuarea controlului intern al ultimului;



- Persoanele fizice, ale căror date cu caracter personal vor fi stocate în Registru;
- Persoanele interesate de a accesa și vizualiza datele din Registru.

5. Angajații Primăriei or. Durlăști poartă răspundere personală pentru îndeplinirea cerințelor prezentului Regulament, asigurarea confidențialității, securității și păstrarea în stare corespunzătoare a informației din Registru.

II. Condiții generale față de ținerea Registrului

6. Registrul de evidență a corespondenței reprezintă un sistem mixt ce utilizează atât evidența în formă electronică, cât și în formă manuală.

7. De către Primăria or. Durlăști va fi asigurată ținerea în formă manuală a unor componente al Registrului (ținând cont de competența funcțională) prin înscrierea informației, inclusiv păstrarea cărții Registrului de către un angajat împuternicit în acest sens (registratorul) din cadrul subdiviziunii respective, în conformitate cu prevederile legislației în vigoare.

8. Obiectul înregistrării reprezintă informația referitor la persoanele care au depus adresări în adresa Primăriei or. Durlăști.

9. Registrul va fi ținut în limba de stat.

10. Registratorul este obligat:

- să introducă în Registru numai informație veridică, colectată de la adresant sau din alte surse neinterzise de lege;
- să asigure evidența în ordine cronologică a fiecărei înscrieri în Registru;
- să nu admită modificarea neîntemeiată a datelor introduse în Registru;
- să efectueze înregistrările în Registru astfel, încât să excludă posibilitatea de a fi radiată (ștersă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ștergerii, distrugerii);
- să asigure accesul la informația din registru doar persoanelor care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare;
- să prevină accesul neautorizat la datele din Registru, utilizarea, difuzarea, modificarea sau nimicirea lor ilegală.

11. Datele din registru vor reflecta starea veridică și actuală a informației privind persoanele vizate în corespondența cu Primăria or. Durlăști.

12. Atât forma manuală, cât și cea electronică a Registrului va cuprinde în mod obligatoriu:

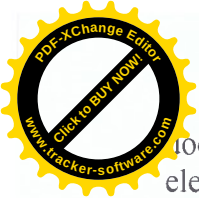
- denumirea Registrului;
- denumirea Primăriei or. Durlăști ca proprietar, posesor și deținător al Registrului;
- numele, prenumele și funcția persoanei responsabile de introducerea datelor în Registru și a administratorului acestuia;
- numele, prenumele și funcția persoanei care va exercita controlul asupra ținerii Registrului;
- numărul Registrului, termenele de ținere și păstrare a acestuia.

13. Datele cu caracter personal din Registru vor fi prelucrate în condițiile stabilite de legislația privind protecția datelor cu caracter personal. În acest sens, vor fi realizate măsuri de asigurare a gradului de exactitate a datelor registrului și de protecție a acestora contra distrugerii întâmplătoare sau neautorizate, modificării, dezvăluirii sau oricăror alte acțiuni ilegale la ținerea registrului.

III. Condiții generale privind introducerea informației în Registru

14. Informația privind corespondența parvenită în adresa Primăriei or. Durlăști, va fi recepționată și înregistrată în aceeași zi de persoana responsabilă din cadrul Primăriei or. Durlăști în Registrul de evidență a corespondenței și după caz, în fișele de evidență și control a acestora, iar versiunea electronică parvenită se înregistrează în arhiva electronică.

15. Înregistrarea informației în Registru se face prin introducerea mențiunilor necesare în cartea de înregistrări (forma manuală) și în Sistemul informatic (forma electronică) în baza datelor furnizate prin



documentele transmise atât de furnizorul datelor registrului, atât pe suport de hîrtie sau în electronică, perfectate în modul stabilit de lege.

16. La înregistrarea corespondenței, pe prima pagină se va aplica ștampila de înregistrare în care se indică data primirii și indicele de înregistrare. Indicele de înregistrare constă după caz, din litera inițială a numelui și prenumelui adresantului, numărul și anul de înregistrare a înscrisului.

17. După caz, se va întocmi manual fișa de evidență și control pentru fiecare adresare (în condițiile stabilite prin Instrucțiunile privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărîrea Guvernului nr. 208 din 31 martie 1995), introducîndu-se datele cu caracter personal ce vizează petiționarul (nume, prenume, adresa de domiciliu, numărul de telefon) precum și rezoluția conducerii Primăriei or. Durlăști, termenul de soluționare stabilit, datele despre starea executării etc.

18. După examinarea și soluționarea definitivă, pe fișa de evidență și control se aplică semnătura persoanei responsabile de evidență, iar în Sistemul informatic se face mențiunea despre finalizarea acesteia și modificarea statutului ca arhivată.

19. Modificările și radierile făcute în Registru se efectuează în baza deciziei și cu semnătura registratorului în situația existenței unui motiv întemeiat în acest sens.

20. Dacă furnizorul datelor registrului se adresează cu un demers argumentat privind rectificarea datelor eronate sau inexacte, registratorul va face, în modul stabilit, corectările necesare și va informa despre aceasta furnizorul datelor.

21. Greșelile de ordin tehnic comise de către persoana împuternicită de ținerea Registrului se rectifică de către aceasta. Corectarea greșelii se specifică într-o rubrică aparte, urmată de semnătura persoanei care a efectuat înscirirea.

22. Radierea obiectului din Registru se face prin inserarea unei note speciale (care trebuie să conțină semnăturile persoanei responsabile și data radierii) și nu reprezintă excluderea fizică a datelor despre obiect din Registru.

23. Rectificările și radierile înscrisurilor din Registru se efectuează astfel încît textul inițial să fie citabil.

IV. Condiții generale privind păstrarea și furnizarea informației din Registru

24. Păstrarea Registrului este asigurată de registrator pînă la adoptarea deciziei conducerii Primăriei or. Durlăști despre lichidarea registrului, dar nu mai mult decît pe perioada stabilită de Indicatorul documentelor-tip și al termenelor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016.

25. Ținerea Registrului este supusă controlului intern și extern, în conformitate cu prevederile art. 31 al Legii cu privire la registre.

26. În acest sens, persoana împuternicită de ținerea și păstrarea Registrului este obligată:

- să prevină accesul nesancționat la datele stocate în Registru;
- să întreprindă acțiuni în vederea neadmiterii cazurilor de utilizare ilegală, dezvăluire ilegală a informației conținute în acesta, de modificare sau nimicire a acestor date.

27. Persoanele împuternicite de ținerea și controlul registrului sînt obligate să nu divulge informația la care au primit acces în legătură cu exercitarea atribuțiilor funcționale, inclusiv după încetarea activității în cadrul Primăriei or. Durlăști.

28. Registratorul este obligat să asigure accesul la informația din registru pentru angajații autorizați ai Primăriei or. Durlăști și alte persoane, care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare sau care demonstrează dreptul și interesul legitim de a primi aceste informații, din momentul în care acestea vor fi disponibile, dar nu mai tîrziu de 5 zile lucrătoare de la data depunerii cererii.

29. Informația poate fi furnizată gratuit sau contra plată în conformitate cu Legea privind accesul la informație.

30. Extrasul din Registru trebuie să fie semnat de conducerea Primăriei or. Durlești, cu în data întocmirii/eliberării acestuia.

V. Condițiile suplimentare privind gestionarea Registrului în forma manuală

31. Ținerea manuală a Registrului de evidență a corespondenței se efectuează sub formă de fișier sau prin introducerea mențiunilor în cartea pentru înregistrări.

32. În acest sens, evidența corespondenței în cadrul Primăriei or. Durlești este dusă prin intermediul mai multor Registre ținute în formă manuală, cum ar fi:

- „Registrul de intrare și ieșire a petițiilor adresate APL Durlești, gestionate de persoana desemnată din cadrul Primăriei or. Durlești;
- „Registrul de intrare/ieșire a corespondenței”, gestionat de persoana desemnată din cadrul Primăriei or. Durlești;
- „Registrul de intrare/ieșire a corespondenței”, gestionat de persoana desemnată din cadrul Primăriei or. Durlești;

33. Registratorul, suplimentar la cele expuse în Cap. IV, în cazul gestionării Registrului în formă manuală, este obligat:

- să efectueze înscrierile citeț și clar. Prescurtările vor fi făcute astfel pentru a fi evitate diferite interpretări. Textul greșit se taie cu o linie, fiind posibilă citirea textului greșit înscris.
- să nu înlocuiască neîntemeiat filele din cartea registrului prin extragerea lor, încheierea unor noi file etc;
- să asigure, în cazul deteriorării cărții, posibilitatea restabilirii imediate a datelor din registru fără a cauza daune informației, ce se conține în ea;
- să asigure șnuruirea cărților pentru înregistrări (în caz că nu este o carte integrală) și numerotarea filelor. Numărul de file se indică pe ultima pagină și se autentifică (inclusiv conținutul cărții) prin aplicarea semnelor de control de către conducerea Primăriei or. Durlești: semnătura și ștampila.

34. Informația va fi introdusă în Registru în ordine cronologică, ținându-se cont de necesitatea prezenței mențiunilor privind:

- numărul de ordine a mențiunii;
- numărul și data de intrare;
- numele și prenumele;
- conținutul succint al documentului;
- numele și prenumele executantului, termenul de executare și rezoluția conducerii Primăriei or. Durlești;
- rezultatul examinării: admisă/respinsă/oferte explicații de rigoare/acte de reacționare adoptate de conducerea Primăriei or. Durlești.

35. Registrul se păstrează de persoana responsabilă într-un safeu metalic și va conține un compartiment separat în care se vor consemna înregistrările de audit a securității, prevăzute de pct. 93 al Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

VI. Condiții suplimentare privind gestionarea Registrului în formă electronică

37. Ținerea în formă electronică a Registrului de evidență a corespondenței este realizat de Primăria or. Durlești prin intermediul unui sistemul informațional automatizat special constituit.

38. Introducerea, modificarea și păstrarea informației în acest Registru este asigurată de registratorul desemnat din cadrul Primăriei or. Durlești .

39. La înscrierea informației privind corespondența parvenită, în Registru se inserează și o listă de date despre obiect, inclusiv date cu privire la faptul înregistrării în compartimentele special destinate. și anume:



- tipul adresării;
- data și numărul de intrare;
- termenul de rezolvare și data expirării;
- numele, prenumele adresantului;
- adresa de domiciliu, e-mail (în cazul existenței);
- numărul de telefon fix/mobil;
- conținutul succint al adresării;
- rezoluția conducerii Primăriei or. Durlești;
- persoana responsabilă de control și executorul;
- copia scanată, în format „.pdf” a adresării;
- date privind executarea;
- date privind posibila prelungire (termenul, numărul documentul prin care s-a efectuat prelungirea, informarea adresantului;
- rezultatul examinării: admisă/respinsă/oferite explicații de rigoare/acte de reacționare adoptate de Primăria or. Durlești.

VII. Măsurile de protecție a datelor cu caracter personal prelucrate în registrul de evidență a corespondenței

40. În cazul neutilizării temporare a purtătorilor de informație pe suport de hîrtie sau electronic care conțin date preluate din registrul de evidență a corespondenței, aceștia se păstrează în safeuri care se încuie.

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

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

43. Accesul fizic la mijloacele de reprezentare a informației preluate din registrul de evidență a corespondenței este blocat împotriva vizualizării de către persoane neautorizate.

44. Mijloacele de prelucrare a informațiilor preluate din registrul de evidență a corespondenței sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

45. Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din registrul de evidență a corespondenței din/în perimetrul de securitate se înregistrează într-un registru specializat.

46. Măsurile de protecție a datelor cu caracter personal, prelucrate în registrul de evidență a corespondenței, se înfăptuiesc ținînd cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică și externă.

47. Cerințe speciale față de marcare: toate informațiile ieșite din registrul de evidență a corespondenței, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului 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

48. Accesul în biroul unde este amplasat registrul de evidență a corespondenței 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/sau cheia de la lacătul mecanic.

49. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.

50. Înainte de acordarea accesului fizic la registrul de evidență a corespondenței, se verifică competențele de acces.

51. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă, conform cerințelor prevăzute în instrucțiunile cu privire la ținerea lucrărilor de secretariat.

52. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat registrul de evidență a corespondenței, fiind integrat din punct de vedere fizic.

53. Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat registrul de evidență a corespondenței, din punct de vedere fizic.

54. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.

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

56. Amplasarea registrului de evidență a corespondenței răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

57. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității registrului de evidență a corespondenței, 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 registrul de evidență a corespondenței, inclusiv posibilitatea deconectării oricărui component TI.

58. Computerele, unde este amplasat fizic registrul de evidență a corespondenței, dispun de UPS-uri, care sînt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

59. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din registrul de evidență a corespondenței, sînt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiatul, cablurile de tensiune sînt separate de cele comunicaționale.

60. Securitatea antiincendiară a registrului de evidență a corespondenței: biroul unde este amplasat registrul de evidență a corespondenței este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiară în vigoare.

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

identificarea și autentificarea utilizatorului registrul de evidență a corespondenței

62. Este efectuată identificarea și autentificarea utilizatorilor informațiilor preluate din registrul de evidență a corespondenței și a proceselor executate în numele acestor utilizatori.

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

64. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hîrtie, cu excepția cazului de asigurare a securității păstrării acestora (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

65. Se efectuează modificarea parolelor de fiecare dată cînd sînt depistați indicii unei eventuale compromiteri a sistemului sau parolei.

66. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sînt folosite identificatori și parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege și

schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora. După trei tentative greșite de autentificare, accesul este blocat, în mod automatizat.

67. Se asigură, pentru o perioadă de 1 /un/ an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor și prevenirea folosirii repetate a acestora.

68. 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 3 luni), codurile de identificare și autentificare se revocă sau se suspendă.

69. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în registrul de evidență a corespondenței, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora. Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în registrul de evidență a corespondenței, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 /una/ lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informațiile din registrul de evidență a corespondenței. Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

70. În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieste cu regularitate, maximum la fiecare șase luni și după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la registrul de evidență a corespondenței.

71. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autorizează de persoanele responsabile.

72. Se impun limite în privința persoanelor care au dreptul:

73. să vizualizeze informațiile stocate în registrul de evidență a corespondenței;

74. b) să copieze, să descarce, să șteargă sau să modifice orice informație stocată.

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

76. Orice activitate de dezvăluire a datelor cu caracter personal către terți este documentată și supusă unei analize riguroase în prealabil privind scopul și temeiul legal a intențiilor de dezvăluire a unui anumit volum de date cu caracter personal.

77. Orice încălcare a securității în ceea ce privește registrul de evidență a corespondenței este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

78. Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea registrului de evidență a corespondenței este controlată și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

IX. Auditul securității în sistemele de evidență a documentelor

79. Se organizează generarea înregistrărilor de audit a securității în registrul de evidență a corespondenței pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

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

a) data și timpul tentativei intrării/ieșirii;

b) ID-ul utilizatorului;

c) rezultatul tentativei de intrare/ieșire – pozitivă sau negativă.

81. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din registrul de evidență a corespondenței,



înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:

- a) data și timpul tentativei de pornire;
- b) denumirea/identificatorul programului aplicativ sau al procesului;
- c) ID-ul utilizatorului;
- d) rezultatul tentativei de pornire – pozitivă sau negativă.

82. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din registrul de evidență a corespondenței, conform următorilor parametri:

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

83. Se efectuează înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

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

84. Se efectuează înregistrarea ieșirii din registrul de evidență a corespondenței, înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:

- a) data și timpul eliberării;
- b) denumirea informației și căile de acces la aceasta;
- c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
- d) ID-ul utilizatorului care a solicitat informația;
- e) volumul documentului eliberat (numărul paginilor, fișierelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.

85. Cazurile de deranjament al auditului securității în registrul de evidență a corespondenței sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoștința persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

86. Rezultatele auditului securității în registrul de evidență a corespondenței (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

87. Durata minimă a stocării rezultatelor auditului securității în registrul de evidență a corespondenței constituie 2 /doi/ ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigațiile sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

X. Asigurarea integrității informațiilor din registrul de evidență a corespondenței

88. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din registrul de evidență a corespondenței, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestora, 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.



89. Se utilizează tehnologii și mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor și constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informațiilor din a registrul de evidență a corespondenței.

90. Se asigură testarea funcționării corecte a componentelor de securitate a registrul de evidență a corespondenței (automat – la pornirea sistemului, și după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

91. Copiile de siguranță: reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către operator intervalul de timp în care se execută copiile de siguranță a informațiilor din registrul de evidență a corespondenței și soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

XI. Gestionarea incidentelor de securitate a registrul de evidență a corespondenței

92. Persoanele care asigură exploatarea registrul de evidență a corespondenței trec, minimum o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

93. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în registrul de evidență a corespondenței.

94. În cazul producerii incidentelor de securitate persoanele responsabile va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar și să asigure accesul la informațiile necesare relevante obiectului controlului.

95. Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din registrul de evidență a corespondenței poartă răspundere civilă, contravențională și penală.

XII. Dispoziții finale

96. Prezentul Regulament este revizuit și ulterior aprobat de către Primarul or. Durlăști periodic, însă cel puțin o dată în an, precum și la necesitate.

97. Prezentul Regulament se completează cu prevederile legislației în vigoare.

98. Regulamentul este adus la cunoștința angajaților contra semnăturii.

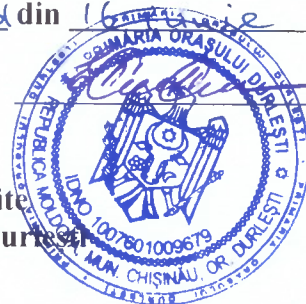
99. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.



Prin Dispoziția Primarului or. Durești
nr. 62 din 16 noiembrie 2021

Aprobat

L.S.



REGULAMENTUL Registrului de evidență a petițiilor parvenite în adresa Administrației Publice Locale a or. Durești

I. Dispoziții generale

1. Regulamentul Registrului de evidență a petițiilor parvenite în adresa P este elaborat în conformitate cu prevederile Codului administrativ al Republicii Moldova, aprobat prin Legea nr. 116 din 19.07.2018, Legii nr. 71-XVI din 22 martie 2007 cu privire la registre, Instrucțiunilor privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 208 din 31 martie 1995, Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010.

2. Prezentul Regulament reglementează modalitatea Ținerii Registrului de evidență a petițiilor parvenite în adresa Administrației Publice Locale a or. Durești (în continuare Registru), precum și procedura de înregistrare, securizare, modificare și radiere a datelor din acest Registru.

3. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută de Legea cu privire la registre, Legea cu privire la petiționare.

Astfel, în sensul prezentului Regulament se definesc următoarele noțiuni:

Petiție - orice cerere, sesizare sau propunere adresată unei autorități publice de către o persoană fizică sau juridică;

Registrul de evidență a petițiilor – resursa informațională specializată (totalitatea informațiilor ținute în formă automatizată și manuală) care asigură evidența informației sistematizate, principalul obiectiv al căruia constă în asigurarea evidenței petițiilor parvenite la Administrația Publice Locale a or. Durești;

Registrator – angajatul Primăriei or. Durești împuternicit cu atribuțiile de introducere, modificare, păstrare a informației din Registru.

Furnizorul datelor - persoana fizică sau reprezentantul persoanei juridice de drept public sau privat, care prezintă registratorului date despre obiectul registrului în modul stabilit de lege sau acord.

4. Subiecți ai raporturilor juridice apărute ca rezultat al instituirii, administrării și Ținerii manuale a Registrului sînt:

- Statul, în calitate de proprietar al Registrului;
- Primăria or. Durești, în calitate de posesor și deținător al Registrului;
- Persoanele împuternicite de Ținerea Registrului și cele responsabile de efectuarea controlului intern al ultimului;
- Petiționarii, ale căror date cu caracter personal vor fi stocate în Registru;
- Persoanele interesate de a accesa și vizualiza datele din Registru.

5. Angajații Primăriei or. Durești poartă răspundere personală pentru îndeplinirea cerințelor prezentului Regulament, asigurarea confidențialității, securității și păstrarea în stare corespunzătoare a informației din Registru.

5.1 Petițiile anonime, înaintate în adresa Administrației Publice Locale a or. Durești, în conformitate cu prevederile art. 76 alin. (1) al Codului administrativ al Republicii Moldova, aprobat prin Legea nr. 116 din 19.07.2018 nu se examinează.



II. Condiții generale față de ținerea Registrului

6. Registrul de evidență a petițiilor reprezintă un sistem mixt ce utilizează atât evidența în formă electronică, cât și în formă manuală.

7. De către Primăria or. Durlăști va fi asigurată ținerea în formă manuală a unor componente al Registrului (ținând cont de competența funcțională) prin înscrierea informației, inclusiv păstrarea cărții Registrului de către un angajat împuternicit în acest sens (registratorul) din cadrul Direcției/Secției respective, în conformitate cu prevederile legislației în vigoare.

8. Persoanele responsabile din cadrul Primăriei or. Durlăști vor asigura suplimentar evidența în formă electronică a petițiilor parvenite în adresa Administrației Publice Locale a or. Durlăști.

9. Obiectul înregistrării reprezintă informația referitor la persoanele care au depus petiții în adresa Administrației Publice Locale a or. Durlăști.

10. Registrul va fi ținut în limba de stat.

11. Registratorul este obligat:

- să introducă în Registru numai informație veridică, colectată de la petiționar sau din alte surse neinterzise de lege;
- să asigure evidența în ordine cronologică a fiecărei înscrieri în Registru;
- să nu admită modificarea neîntemeiată a datelor introduse în Registru;
- să efectueze înregistrările în Registru astfel, încât să excludă posibilitatea de a fi radiată (ștearsă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ștergerii, distrugerii);
- să asigure accesul la informația din registru doar persoanelor care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare;
- să prevină accesul neautorizat la datele din Registru, utilizarea, difuzarea, modificarea sau nimicirea lor ilegală.

12. Datele din registru vor reflecta starea veridică și actuală a informației privind petiționarii ce s-au adresat Administrației Publice Locale a or. Durlăști.

13. Atât forma manuală, cât și cea electronică a Registrului va cuprinde în mod obligatoriu:

- denumirea Registrului;
- Primăria or. Durlăști ca posesor și deținător al Registrului;
- numele, prenumele și funcția persoanei responsabile de introducerea datelor în Registru și a administratorului acestuia;
- numele, prenumele și funcția persoanei care va exercita controlul asupra ținerii Registrului;
- numărul Registrului, termenele de ținere și păstrare a acestuia.

14. Datele cu caracter personal din Registru vor fi prelucrate în condițiile stabilite de legislația privind protecția datelor cu caracter personal. În acest sens, vor fi realizate măsuri de asigurare a gradului de exactitate a datelor registrului și de protecție a acestora contra distrugerii întâmplătoare sau neautorizate, modificării, dezvăluirii sau oricăror alte acțiuni ilegale la ținerea registrului.

III. Condiții generale privind introducerea informației în Registru

15. Informația privind petițiile parvenite în adresa Administrației Publice Locale a or. Durlăști va fi recepționată și înregistrată în aceeași zi de persoana responsabilă din cadrul Primăriei or. Durlăști în Registrul de evidență a petițiilor și în fișele de evidență și control a acestora, iar versiunea electronică parvenită se înregistrează în arhiva electronică a Primăriei or. Durlăști.

16. Înregistrarea informației în Registru se face prin introducerea mențiunilor necesare în cartea de înregistrări (forma manuală) și în sistemul informațional de evidență automatizată a petițiilor „Registrul petițiilor” (forma electronică) în baza datelor furnizate prin documentele transmise atât de furnizorul datelor registrului (petiționarul), atât pe suport de hârtie sau în formă electronică, perfectate în modul stabilit de lege.

17. La înregistrarea petițiilor, pe prima pagină se va aplica ștampila de înregistrare în care se



indică data primirii petiției și indicele de înregistrare. Indicele de înregistrare constă din litera în care este înregistrată petiția, numărul și anul de înregistrare a petiției.

18. Concomitent se va întocmi manual fișa de evidență și control pentru fiecare petiție (în condițiile stabilite prin Instrucțiunile privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 208 din 31 martie 1995), introducându-se datele cu caracter personal ce vizează petiționarul (nume, prenume, adresa de domiciliu, numărul de telefon) precum și rezoluția conducerii Primăriei or. Durlăști, termenul de soluționare stabilit, datele despre starea executării etc.

19. După examinarea și soluționarea definitivă, pe fișa de evidență și control se aplică semnătura persoanei responsabile de evidența petițiilor, iar în baza de date „Registrul petițiilor” se face mențiunea despre finalizarea acesteia și modificarea statutului ca arhivată.

20. Modificările și radierile făcute în Registru se efectuează în baza deciziei și cu semnătura registratorului în situația existenței unui motiv întemeiat în acest sens.

21. Dacă furnizorul datelor registrului se adresează cu un demers argumentat privind rectificarea datelor eronate sau inexacte, registratorul va face, în modul stabilit, corectările necesare și va informa despre aceasta furnizorul datelor.

22. Greșelile de ordin tehnic comise de către persoana împuternicită de ținerea Registrului se rectifică de către aceasta. Corectarea greșelii se specifică într-o rubrică aparte, urmată de semnătura persoanei care a efectuat înscrierea.

23. Radierea obiectului din Registru se face prin inserarea unei note speciale (care trebuie să conțină semnăturile persoanei responsabile și data radierii) și nu reprezintă excluderea fizică a datelor despre obiect din Registru.

24. Rectificările și radierile înscrisurilor din Registru se efectuează astfel încât textul inițial să fie citabil.

IV. Condiții generale privind păstrarea și furnizarea informației din Registru

25. Păstrarea Registrului este asigurată de registrator până la adoptarea deciziei conducerii Primăriei or. Durlăști despre lichidarea registrului, dar nu mai mult de 2 ani, din momentul primei înregistrări, după care informația va fi arhivată sub forma unor date statistice, depersonalizate.

26. Ținerea Registrului este supusă controlului intern și extern, în conformitate cu prevederile art. 31 al Legii cu privire la registre.

27. În acest sens, persoana împuternicită de ținerea și păstrarea Registrului este obligată:

- să prevină accesul nesancționat la datele stocate în Registru;
- să întreprindă acțiuni în vederea neadmiterii cazurilor de utilizare ilegală, dezvăluire ilegală a informației conținute în acesta, de modificare sau nimicire a acestor date.

28. Persoanele împuternicite de ținerea și controlul registrului sînt obligate să nu divulge informația la care au primit acces în legătură cu exercitarea atribuțiilor funcționale, inclusiv după încetarea activității în cadrul Primăriei or. Durlăști.

29. Registratorul este obligat să asigure accesul la informația din registru pentru angajații autorizați ai Primăriei or. Durlăști și alte persoane, care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare sau care demonstrează dreptul și interesul legitim de a primi aceste informații, din momentul în care acestea vor fi disponibile, dar nu mai tîrziu de 5 zile lucrătoare de la data depunerii cererii.

30. Informația poate fi furnizată gratuit sau contra plată în conformitate cu Legea privind accesul la informație.

31. Extrasul din Registru trebuie să fie semnat de conducerea Primăriei or. Durlăști, cu indicarea datei întocmirii/eliberării acestuia.

31.1 Informația extrasă din sistemul de evidență al petițiilor trebuie să fie marcată, conținînd nr. operatorului de date cu caracter personal, sistemul de evidență din care a fost extrasă, precum și avertizarea utilizatorilor acesteia despre obligația prelucrării informației în conformitate cu prevederile Legii privind protecția datelor 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

V. Condițiile suplimentare privind gestionarea Registrului în forma manuală

32. Ținerea manuală a Registrului de evidență a petițiilor se efectuează sub formă de fișier sau prin introducerea mențiunilor în cartea pentru înregistrări.

33. În acest sens, evidența petițiilor în cadrul Primăriei or. Durlești este dusă prin intermediul mai multor Registre ținute în formă manuală, cum ar fi:

- „Registrul de intrare și ieșire a petițiilor adresate Administrației Publice Locale a or. Durlești”, inclusiv „Registrul de ieșire a corespondenței”, gestionate de persoana desemnată din cadrul Primăriei or. Durlești;
- „Registrul de intrare a corespondenței”, gestionat de persoana desemnată din cadrul Primăriei or. Durlești;
- „Registrul de ieșire a corespondenței”, gestionat de persoana desemnată din cadrul Primăriei or. Durlești;

34. Registratorul, suplimentar la cele expuse în Cap. IV, în cazul gestionării Registrului în formă manuală, este obligat:

- să efectueze înscrierile citeț și clar. Prescurtările vor fi făcute astfel pentru a fi evitate diferite interpretări. Textul greșit se taie cu o linie, fiind posibilă citirea textului greșit înscris.
- să nu înlocuiască neintemeiat filele din cartea registrului prin extragerea lor, încheierea unor noi file etc;
- să asigure, în cazul deteriorării cărții, posibilitatea restabilirii imediate a datelor din registru fără a cauza daune informației, ce se conține în ea;
- să asigure șnuruirea cărților pentru înregistrări (în caz că nu este o carte integrală) și numerotarea filelor. Numărul de file se indică pe ultima pagină și se autentifică (inclusiv conținutul cărții) prin aplicarea semnelor de control de către conducerea Primăriei or. Durlești: semnătura și ștampila.

35. Informația va fi introdusă în Registru în ordine cronologică, ținându-se cont de necesitatea prezenței mențiunilor privind:

- numărul de ordine a mențiunii;
- numărul și data de intrare;
- numele și prenumele petiționarului;
- conținutul succint al documentului;
- numele și prenumele executantului, termenul de executare și rezoluția conducerii Primăriei or. Durlești;
- rezultatul examinării petiției: admisă/respinsă/oferte explicații de rigoare/acte de reacționare adoptate de Administrația Publică Locală a or. Durlești.

36. Registrul se păstrează de persoana responsabilă într-un safeu metalic și va conține un compartiment separat în care se vor consemna înregistrările de audit a securității, prevăzute de pct. 93 al Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

VI. Condiții suplimentare privind gestionarea Registrului în formă electronică

37. Ținerea în formă electronică a Registrului de evidență a petițiilor este realizat de Primăriei or. Durlești prin intermediul unui sistem informațional automatizat special constituit - „Registrul petițiilor”.

38. Introducerea, modificarea și păstrarea informației în acest Registru este asigurată de



registratorul desemnat din cadrul - Primăriei or. Durllești;

39. La înscrierea informației privind petiția parvenită, în Registru se inserează și o listă cu date despre obiect, inclusiv date cu privire la faptul înregistrării în compartimentele special destinate, și anume:

- tipul petiției;
- data și numărul de intrare;
- termenul de rezolvare și data expirării;
- numele, prenumele petiționarului;
- adresa de domiciliu, e-mail (în cazul existenței);
- numărul de telefon fix/mobil;
- conținutul succint al petiției;
- rezoluția conducerii Primăriei or. Durllești;
- persoana responsabilă de control și executorul;
- copia scanată, în format „.pdf” a petiției;
- date privind executarea;
- date privind posibila prelungire (termenul, numărul documentul prin care s-a efectuat prelungirea, informarea petiționarului;
- rezultatul examinării petiției: admisă/respinsă/oferte explicații de rigoare/acte de reacționare adoptate de Administrația Publică Locală a or. Durllești.

40. Sistemul informațional de evidență a petițiilor „Registru petițiilor” va fi gestionat, pe toată perioada ciclului de viață, în conformitate cu prevederile stabilite de Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, în special pct. 11-13, 22, 24, 26, 28, 30, 32-33, 35-37, 39-73, 75-78, 85-86, 88, 90.