REPUBLICA MOLDOVA
RAIONUL CĂLĂRAȘI
CONSILIUL COMUNAL TIBIRICA

MD-4441, Republica Moldova, raionul Călăraşi, comuna Ţibirica,
str. Botanica 1, tel.0244 65238, tel/fax. 0244 65236, primariatibirica2018@mail.ru

D E C I Z I A nr. 08/14
din 09 decembrie 2021

„Cu privire la aprobarea Politicii de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Primăria Țibirica"

Examinând notă informativă cu privire la aprobarea Politicii de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale, prezentată de dna Fărîmă Ala, secretar al consiliului comunal;

În temeiul art.14 al Legii nr.436-XVI din 28.12.2006 privind administrația publică locală,

Legii nr.133 din 08.07.2011 privind protecția datelor cu caracter personal,

În conformitate cu Regulamentul Registrului de evidență al operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului Republicii Moldova nr.296 din 15.05.2012,

Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010;

În baza Regulamentului privind constituirea şi funcţionarea Consiliului conumal Ţibirica, aprobat prin decizia Consiliului comunal nr.06/01 din 25 iulie 2015;

Avizului comisiei de specialitate pe problemele sociale,

Consiliul comunal DECIDE:

1. Se aprobă Politica de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Primăria Țibirica, conform Anexei nr.1 la prezenta decizie.
2. Se aprobă Regulamentul Registrului de evidență al petițiilor parvenite în adresa Primăriei Țibirica, conform Anexei nr.2 la prezenta decizie.
3. Se aprobă Regulamentul privind condițiile generale și cerințele față de prelucrarea datelor cu caracter personal în gestionarea resurselor umane, conform Anexei nr.3 la prezenta decizie.
4. Se aprobă Regulamentul privind condițiile generale și cerințele față de prelucrarea datelor cu caracter personal în gestionarea sistemelor de evidență contabilă ale Primăriei Țibirica, conform Anexei nr.4 la prezenta decizie.
5. Executarea prezentei Decizii se atribuie persoanelor responsabile de Politica de securitate a datelor cu caracter personal.
6. Controlul asupra executării prezentei decizii i se atribuie dlui Iurcu Ion, primarul comunei.

Au votat: „pentru" – 9, "contra" – 0, "s-au abţinut" – 0.

Președintele ședinței
contrasemnat:
Secretar al consiliului

Ex: Fărîmă Ala,
secretar al consiliului
Tel:024465238

Anexa nr.1
la decizia consiliului local
nr.08/14 din 09.12.2021

POLITICA DE SECURITATE

PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR INFORMAȚIONALE GESTIONATE DE PRIMĂRIA ȚIBIRICA, RAIONUL CĂLĂRAȘI

I. PREAMBUL:

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

- Declarația universală a drepturilor omului;
- Convenția pentru apărarea drepturilor omului și a libertăților fundamentale;
- Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal și a actelor **naționale:**
- Constituția Republicii Moldova;
- Legea privind protecția datelor cu caracter personal;
- Legea privind accesul la informație;
- 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;
- Regulamentului Registrului de evidență al operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012;
- alte acte legislative/normative de profil.

II. INTRODUCERE:

Primăria comunei Țibirica, are sediul înregistrat în raionul Călărași, satul Țibirica. Politica este aprobată de către Consiliul comunal Țibirica, care acționează în baza legislației: Codul de procedură civilă al Republicii Moldova, Legea nr. 436 din 28.12.2006 privind administrația publică locală, Codul Muncii al Republicii Moldova. Prezenta Politică este aprobată, inclusiv, în vederea conformării activității Primăriei Țibirica cu prevederile Hotărârii Guvernului Republicii Moldova nr.1123 din 14 decembrie 2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal și Legii Republicii Moldova nr.133 din 08.07.2011 privind protecția datelor cu caracter personal.

III. NOȚIUNI GENERALE:

În prezenta Politică de Securitate, sunt definite/utilizate următoarele noțiuni:

date cu caracter personal – orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

categorii speciale de date cu caracter personal – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancțiunile contravenționale;

operator – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;

persoană împuternicită de către operator – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator;

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

control de securitate – acțiuni întreprinse de către Primăria Țibirica, în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;

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

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

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

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

nivel de protecţie – nivel de securitate proporţional riscului pe care îl comportă prelucrarea faţă de datele cu caracter personal respective, precum şi faţă de drepturile şi libertăţile persoanelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestora;

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

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

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

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

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

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

tehnologie informaţională – totalitatea metodelor, procedeelor şi mijloacelor de prelucrare, şi transmitere a informaţiei care conţine date cu caracter personal, şi regulile de aplicare a acesteia;

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

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

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

prelucrarea datelor cu caracter personal – orice operaţiune sau serie de operaţiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;

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

sistem de evidenţă a datelor cu caracter personal – orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcţionale sau geografice;

consimţământul subiectului datelor cu caracter personal – orice manifestare de voinţă liberă, expresă şi necondiţionată, în formă scrisă sau electronică, conform cerinţelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;

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

IV. OBIECTIVILE POLITICII DE SECURITATE:

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de Primăria Ţibirica, Consiliul local Ţibirica, atât în cadrul prelucrării manuale, cât şi sistemelor şi proceselor de tehnologie informaţională. Securitatea reprezintă o componentă esenţială a derulării optime a proceselor bazate pe IT în cadrul Primăriei Ţibirica. Baza unei securităţi IT adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datele cu caracter personal, sistemelor şi proceselor IT împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislaţiei. Având în vedere că siguranţa IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic şi de altă natură.

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

Reglementările prezentei Politici reprezintă un standard minim pentru Primăria Ţibirica, inclusiv toţi angajaţii instituţiilor publice din subordine.

Pornind de la această reglementare, toţi angajaţii Primăriei Ţibirica şi instituţiilor din subordine urmează să respecte strict prevederile Politicii şi regulilor interne ale Primăriei Ţibirica privind protecţia datelor cu caracter personal şi sistemelor IT.

V. DISPOZIŢII PRIVIND IERARHIA ŞI RESPONSABILITATEA PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE:

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

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

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

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

Persoana responsabilă desemnată, indiferent de funcţiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit primarului comunei Ţibirica, raionul Călăraşi, sau persoanei care îndeplineşte interimatul funcţiei.

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

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

VI. MIJLOACELE SUPUSE PRINCIPIILOR DE PROTECȚIE A DATELOR CU CARACTER PERSONAL:

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

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

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

VII. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL SÎNT ASIGURATE ÎN SCOPUL:

- preîntâmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;
- neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- eficientizarea resurselor informaționale atât pe suport de hîrtie cât şi cel în format electronic.
-

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

- preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
- preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
- preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea canalelor VPN;
- preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă;
- preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent;

- stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni cât și pentru cei externi.

IX. PROCEDURILE ORGANIZATORICE ȘI TEHNICE CARE URMEAZĂ A FI RESPECTATE ÎN CADRUL CONSILIULUI RAIONAL LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

1. Măsurile generale de administrare a securității informaționale:

a) În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.

b) Computerele, terminalele de acces și imprimantele sunt deconectate la terminarea sesiunilor de lucru.

c) Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.

d) Este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

e) Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.

f) Toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere.

g) Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

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

a) Accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).

b) Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.

c) Perimetrul de securitate al Primăriei Țibirica și instituțiilor din subordine reprezintă perimetru oficiilor în care se prelucrează/stochează date cu caracter personal.

d) Perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sunt rezistenți, intrările sunt echipate cu lacăte și semnalizare.

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

f) Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc membrii.

g) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

h) Accesul în perimetrul de securitate a clădirii Primăriei Țibirica, unde se prelucrează/ stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținând cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 ale Legii privind protecția datelor cu caracter personal, precum și pct. 26 din Cerințe.

i) Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței unei permisiuni speciale a conducerii.

3. Identificarea şi autentificarea utilizatorilor

a) Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.

b) Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conţine semnalmentele nivelului de accesibilitate al utilizatorului.

c) Pentru confirmarea ID-ului utilizatorului sunt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.

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

4. Identificarea şi autentificarea echipamentului

Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal, cu menţinerea acestor informaţii pentru o perioadă îndelungată.

5. Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:

- identificarea univocă a fiecărui utilizator;
- verificarea autenticităţii fiecărui utilizator.

6. Utilizarea parolelor în procesul asigurării securităţii informaţionale

Sunt respectate regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:

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

7. Controlul administrării accesului

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

8. Accesul de la distanţă

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

b) Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este autorizată de persoanele responsabile ale Primăriei Ţibirica şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

9. Limitarea folosirii tehnologiilor fără fir

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

b) Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.

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

10. Securitatea electroenergetică

a) Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.

b) În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

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

11. Controlul instalării şi scoaterii componentelor T.I.

a) Este exercitat controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal.

b) Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitându-se folosirea funcţiilor standarde de nimicire.

12. Dezvăluirea datelor cu caracter personal

a) Dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidență, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidenţă a datelor cu caracter personal este permis doar utilizatorilor autorizaţi. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieşind din posibilităţile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi. În cazul în care reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere *(expediere poştală cu aviz recomandat, înmânarea personală, etc.*).

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

c) Sunt interzise operaţiunile de dezvăluire a datelor cu caracter personal între Primăria Țibirica şi alte entităţi care sunt amplasate geografic în stânga Nistrului care refuză să se supună juridic legislaţiei Republicii Moldova, reieşind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecţia datelor cu caracter personal.

d) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hârtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luându-se în considerare necesitatea asigurării unui nivel adecvat de protecţie a datelor cu caracter personal.

e) Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecţia datelor cu caracter personal, în

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

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

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

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

Urmează a ţine cont de faptul că în conformitate cu prevederile art.8 al Legii privind accesul la informaţie, datele cu caracter personal fac parte din categoria informaţiei oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislaţiei privind protecţia datelor cu caracter personal.

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoştinţă cu fişa personală a clientului, aceştia urmează a fi informaţi în scris despre obligaţiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 şi 30 ale Legii privind protecţia datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 74^1 Cod contravenţional.

13. Drepturile subiecţilor de date cu caracter personal

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

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

b) Subiecţilor de date cu caracter personal le este asigurat dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu

caracter personal ce vizează alți subiecți, conținute în fișele personale *(alte materiale),* cu excepția cazurilor în care solicitanții își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.

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

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

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

a) Accesul în spațiile/perimetrul unde sunt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform Politicii de securitate aprobată de Consiliul local Țibirica.

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

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

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

15. Auditul sistemelor informaționale gestionate

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

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

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

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

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

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

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

- data și timpul eliberării;

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

16. Asigurarea protecţiei contra programelor dăunătoare (virusilor)

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

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

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

18. Gestionarea incidentelor de securitate

a) Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

b) Personalul Primăriei Țibirica informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

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

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

e) În cazul producerii incidentelor de securitate în cadrul Primăriei Țibirica, persoana resposabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi 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.

f) În cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar şi asigurat accesul la informațiile necesare relevante obiectului controlului.

19. Marcarea documentelor

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

20. Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum şi a informațiilor cu accesibilitate limitată

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă, contravențională sau penală.

Secretar al consiliului comunal Țibirica **FĂRÎMĂ Ala**

ANEXA nr.2
la Decizia Consiliului local
nr. 08/14 din 09 decembrie 2021

REGULAMENTUL
REGISTRULUI DE EVIDENȚĂ A PETIȚIILOR PARVENITE ÎN ADRESA PRIMĂRIEI ȚIBIRICA RAIONUL CĂLĂRAȘI

I. Dispoziţii generale:

1. Regulamentul Registrului de evidenţă a petiţiilor parvenite în adresa Primăriei Țibirica raionul Călăraşi 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, Instrucţiunilor privind ţinerea lucrărilor de secretariat referitoare la petiţiile persoanelor fizice şi juridice, adresate organelor de stat, întreprinderilor, instituţiilor şi organizaţiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 208 din 31 martie 1995, Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010.

2. Prezentul Regulament reglementează modalitatea ţinerii Registrului de evidenţă a petiţiilor parvenite în adresa Primăriei Țibirica și și instituțiilor din subordine (în continuare Registru), precum şi procedura de înregistrare, securizare, modificare şi radiere a datelor din acest Registru.

3. Noţiunile utilizate în prezentul Regulament au semnificaţia prevăzută de Codului Administrativ al Republicii Moldova şi Legea cu privire la registre.

Astfel, în sensul prezentului Regulament se definesc următoarele noţiuni:

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

Registrul de evidenţă a petiţiilor – resursa informaţională specializată (totalitatea informaţiilor ţinute în formă manuală) care asigură evidenţa informaţiei sistematizate, principalul obiectiv al căruia constă în asigurarea evidenţei petiţiilor parvenite la Primăria Țibirica;

Registrator – angajatul Primăriei Țibirica, din cadrul aparatului primarului, împuternicit cu atribuţiile de introducere, modificare, păstrare a informaţiei 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. Subiecţi ai raporturilor juridice apărute ca rezultat al instituirii, administrării şi ţinerii manuale a Registrului sunt:

- Statul, în calitate de proprietar al Registrului;
- Primăria Țibirica, în calitate de posesor şi deţinător al Registrului;
- Persoanele împuternicite de ţinerea Registrului şi cele responsabile de efectuarea controlului intern al ultimului;
- Petiţionarii, ale căror date cu caracter personal vor fi stocate în Registru;
- Persoanele interesate de a accesa şi vizualiza datele din Registru.

5. Angajații Primăriei Țibirica poartă răspundere personală pentru îndeplinirea cerinţelor prezentului Regulament, asigurarea confidenţialităţii, securităţii şi păstrarea în stare corespunzătoare a informaţiei din Registru.

5.1 Petiţiile anonime sau cele depuse fără indicarea adresei poştale sau electronice a petiționarului înaintate în adresa Primăriei Țibirica, în conformitate cu prevederile art. 76 alin. (1) al Codului Administrativ al RM, aprobat prin Legea nr. 116 din 19.07.2019 nu se examinează.

II. Condiţii generale faţă de ţinerea Registrului:

6. Registrul de evidenţă a petiţiilor reprezintă un sistem de evidenţă în formă manuală.

7. De către reprezentanţii primăriei Ţibirica va fi asigurată ţinerea în formă manuală a unor componente ale Registrului (ţinând cont de competenţa funcţională) prin înscrierea informaţiei, inclusiv păstrarea cărţii Registrului de către un funcţionar public împuternicit în acest sens (registratorul) din cadrul primăriei respective, în conformitate cu prevederile legislaţiei în vigoare.

8. Obiectul înregistrării reprezintă informaţia referitor la persoanele care au depus petiţii în adresa Primăriei Ţibirica.

9. Registrul va fi ţinut în limba de stat.

10. Registratorul este obligat:
- să introducă în Registru numai informaţie veridică, colectată de la petiţionar sau din alte surse neinterzise de lege;
- să asigure evidenţa 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 (ştearsă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ştergerii, distrugerii);
- să asigure accesul la informaţia din Registru doar persoanelor care au dreptul de a primi informaţia respectivă, în conformitate cu legislaţia 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 şi actuală a informaţiei privind petiţionarii ce s-au adresat Primăriei Ţibirica.

12. Registrul va cuprinde următoarele elemente:
- denumirea Registrului;
- denumirea "Primăria Ţibirica" ca posesor şi deţinător al Registrului;
- numele, prenumele şi funcţia persoanei responsabile de introducerea datelor în Registru şi a administratorului acestuia;
- numele, prenumele şi funcţia persoanei care va exercita controlul asupra ţinerii Registrului;
- numărul Registrului, termenele de ţinere şi păstrare a acestuia.

13. Datele cu caracter personal din Registru vor fi prelucrate în condiţiile stabilite de legislaţia privind protecţia datelor cu caracter personal. În acest sens, vor fi realizate măsuri de asigurare a gradului de exactitate a datelor Registrului şi de protecţie a acestora contra distrugerii întâmplătoare sau neautorizate, modificării, dezvăluirii sau oricăror alte acţiuni ilegale la ţinerea Registrului.

III. Condiţii generale privind introducerea informaţiei în Registru:

14. Informaţia privind petiţiile parvenite în adresa Primăriei Ţibirica va fi recepţionată şi înregistrată în aceiaşi zi de persoana responsabilă din cadrul primăriei în Registrul de evidenţă a petiţiilor şi în fişele de evidenţă şi control a acestora.

15. Înregistrarea informaţiei în Registru se face prin introducerea menţiunilor necesare în cartea de înregistrări în baza datelor furnizate prin documentele transmise atât de furnizorul datelor Registrului (petiţionarul), perfectate în modul stabilit de lege.

16. La înregistrarea petiţiilor, pe prima pagină se va aplica ştampila de înregistrare în care se indică data primirii petiţiei şi indicele de înregistrare. Indicele de înregistrare constă din litera iniţială a numelui şi prenumelui petiţionarului, numărul şi anul de înregistrare a petiţiei.

17. Concomitent se va întocmi fişa de evidenţă şi control pentru fiecare petiţie (în condiţiile stabilite prin Instrucţiunile privind ţinerea lucrărilor de secretariat referitoare la petiţiile persoanelor fizice şi juridice, adresate organelor de stat, întreprinderilor, instituţiilor şi organizaţiilor Republicii Moldova, aprobate prin Hotărîrea Guvernului nr. 208 din 31 martie 1995), introducându-se datele cu caracter personal ce vizează petiţionarul (nume, prenume, adresa de domiciliu, numărul de

telefon) precum şi rezoluţia conducerii primăriei Ţibirica, termenul de soluţionare stabilit de conducerea primăriei, datele despre starea executării etc.

18. După examinarea şi soluţionarea definitivă, pe fişa de evidenţă şi control se aplică semnătura persoanei responsabile de evidenţa petiţiilor, iar în baza de date "Registrul petiţiilor" se face menţiunea despre finalizarea acesteia şi modificarea statutului ca arhivată.

19. Modificările şi radierile făcute în Registru se efectuează în baza deciziei şi cu semnătura registratorului în situaţia existenţei 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 şi va informa despre aceasta furnizorul datelor.

21. Greşelile de ordin tehnic comise de către persoana împuternicită de ţinerea Registrului se rectifică de către aceasta. Corectarea greşelii se specifică într-o rubrică aparte, urmată de semnătura persoanei care a efectuat înscrierea.

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

23. Rectificările şi radierile înscrisurilor din Registru se efectuează astfel încît textul iniţial să fie citabil.

IV. Condiţii generale privind păstrarea şi furnizarea informaţiei din Registru:

24. Păstrarea Registrului este asigurată de registrator până la adoptarea deciziei Consiliului local despre lichidarea Registrului, dar nu mai mult de 3 ani, din momentul primei înregistrări, după care informaţia va fi arhivată sub forma unor date statistice, depersonalizate.

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

26. În acest sens, persoana împuternicită de ţinerea şi păstrarea Registrului este obligată:
- să prevină accesul nesancţionat la datele stocate în Registru;
- să întreprindă acţiuni în vederea neadmiterii cazurilor de utilizare ilegală, dezvăluire ilegală a informaţiei conţinute în acesta, de modificare sau nimicire a acestor date.

27. Persoanele împuternicite de ţinerea şi controlul Registrului sunt obligate să nu divulge informaţia la care au primit acces în legătură cu exercitarea atribuţiilor funcţionale, inclusiv după încetarea activităţii în cadrul Primăriei Ţibirica.

28. Registratorul este obligat să asigure accesul la informaţia din Registru pentru angajaţii autorizaţi ai Primăriei Ţibirica şi alte persoane, care au dreptul de a primi informaţia respectivă, în conformitate cu legislaţia în vigoare sau care demonstrează dreptul şi interesul legitim de a primi aceste informaţii, din momentul în care acestea vor fi disponibile, dar nu mai târziu de 5 zile lucrătoare de la data depunerii cererii.

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

30. Extrasul din Registru trebuie să fie semnat de conducerea Primăriei Ţibirica, cu indicarea datei întocmirii/eliberării acestuia.

31. Informaţia extrasă din sistemul de evidenţă al petiţiilor trebuie să fie marcată, conţinând nr. operatorului de date cu caracter personal, sistemul de evidenţă din care a fost extrasă, precum şi avertizarea utilizatorilor acesteia despre obligaţia prelucrării informaţiei în conformitate cu prevederile Legii privind protecţia datelor cu caracter personal.

V. Condiţiile suplimentare privind gestionarea Registrului:

32. Ţinerea manuală a Registrului de evidenţă a petiţiilor se efectuează sub formă de fişier sau prin introducerea menţiunilor în cartea pentru înregistrări.

33. În acest sens, evidenţa petiţiilor în cadrul Primăriei Ţibirica este dusă prin intermediul mai multor Registre ţinute în formă manuală, cum ar fi:

- "Registrul de intrare şi ieşire a petiţiilor adresate Primăriei Ţibirica şi Consiliului local", inclusiv;
- "Registrul de ieşire a corespondenţei", gestionat de persoana desemnată din cadrul Primăriei Ţibirica;
- "Registrul de intrări locale a petiţiilor", gestionat de persoana desemnată din cadrul Primăriei Ţibirica;

34. Registratorul, suplimentar la cele expuse în Capitolul IV, în urma gestionării Registrului, este obligat:

- să efectueze înscrierile citeţ şi clar. Prescurtările vor fi făcute astfel pentru a fi evitate diferite interpretări. Textul greşit se taie cu o linie, fiind posibilă citirea textului greşit înscris.
- să nu înlocuiească neintemeiat filele din cartea Registrului prin extragerea lor, încleierea unor noi file etc;
- să asigure, în cazul deteriorării cărţii, posibilitatea restabilirii imediate a datelor din Registru fără a cauza daune informaţiei, ce se conţine în ea;
- să asigure şnuruirea cărţilor pentru înregistrări (în caz că nu este o carte integrală) şi numerotarea filelor. Numărul de file se indică pe ultima pagină şi se autentifică (inclusiv conţinutul cărţii) prin aplicarea semnelor de control de către conducerea Primăriei Ţibirica: semnătura şi ştampila.

35. Informaţia va fi introdusă în Registru în ordine cronologică, ţinându-se cont de necesitatea prezenţei menţiunilor privind:

- numărul de ordine a menţiunii;
- numărul şi data de intrare;
- numele şi prenumele petiţionarului;
- conţinutul succint al documentului;
- numele şi prenumele executantului, termenul de executare şi rezoluţia conducerii Primăriei;
- rezultatul examinării petiţiei: admisă/respinsă/oferite explicaţii de rigoare/acte de reacţionare adoptate de Primăria Ţibirica /Consiliul local Ţibirica.

36. Registrul se păstrează de persoana responsabilă într-un safeu metalic şi va conţine un compartiment separat în care se vor consemna înregistrările de audit a securităţii, prevăzute de pct. 93 al Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

Secretar al consiliului comunal Ţibirica **FĂRÎMĂ Ala**

ANEXA nr.3
la Decizia Consiliului local
nr. 08/14 din 09 decembrie 2021

REGULAMENTUL PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL ÎN GESTIONAREA RESURSELOR 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 Primăriei Țibirica 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 Hotărîrea 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 Primăriei Țibirica și instituțiilor din subordine ale acesteia de către persoanele responsabile de resurse umane.

II. SCOPUL

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul resurse umane constă în:

- înregistrarea și evidența personalului;
- controlul și analiza calitativă a completării statului de personal;
- evidență și analiză a:
  - formelor de angajare și modalități de obținere a funcțiilor, posturilor de muncă;
  - vârstei, sexului, studiilor și cunoștințelor, originei și stării sociale, stagiului de muncă etc.;
  - deplasărilor, concediilor;
  - concedierilor, inclusiv motivațiilor.
- sancțiuni disciplinare/stimulări pentru succese în muncă;
- selectarea datelor referitoare la angajați conform criteriilor stabilite, perfectarea documentelor respective.

2.1.1. De persoana responsabilă de sistemul resurse umane sunt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele și patronimicul;
- sexul;
- data și locul nașterii;
- semnătura;
- datele din actele de stare civilă;
- codul asigurării medicale (CPAM);
- telefon mobil;
- e-mail;
- profesie, funcție;
- formarea profesională (diplome, studii);
- situație familială;
- datele membrilor de familie;
- cetățenia;
- semnătura digitală;
- date din permisul de conducere;
- sacțiuni disciplinare;

- codul personal de asigurări sociale (CPAS);
- telefon /fix;
- adresa (domiciliului/reședinței);
- loc de muncă;
- numărul personal de identificare de stat (IDNP);
- situație militară;
- situație economică sau financiară;
- imagine;
- obișnuințe/preferințe/comportament;
- Altele (mărimea salariului, premii, stimulări, suplimente, date din certificatul medical).

2.2. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către Operator astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. 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 Primăriei Țibirica și instituțiilor din subordine, și care au impact asupra calculării plăților salariale;

b) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor de incapacitate temporară de muncă;

c) Prelucrarea copiilor ordinelor/dispozițiilor conducerii referitoare la personal.

2.3. Orice utilizare a datelor cu caracter personal, introduse în sistemul resurse umane în alte scopuri decât cele menționate mai sus este interzisă.

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI RESURSE UMANE

3.1. Datele cu caracter personal ale angajaților Primăriei Țibirica și instituțiilor din subordine se prelucrează/stochează pe suport de hârtie.

3.2. Prelucrarea informațiilor pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri, care sunt amplasate fizic în biroul persoanei responsabile de gestionarea sistemului resurse umane.

IV. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal de persoana responsabilă de gestionarea sistemului resurse umane se efectuează pe perioada activității angajaților Primăriei Țibirica și instituțiilor din subordine (din momentul semnării contractului până la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă). Formularul de participare la concurs a potențialilor angajați se păstrează în format arhivat conform Nomenclatorului dosarelor din cadrul Primăriei Țibirica.

4.2. La expirarea termenelor menționate în punctul 4.1, datele sunt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul dosarelor din cadrul Primăriei Țibirica aprobat de primarul localității, f/n, ulterior fiind supuse distrugerii sau transmiterii în arhiva raională.

V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. Primăria Țibirica, 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;
- de a se adresa în instanța de judecată.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din domeniul resurse umane 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 primarului sau sau conducătorului instituției din subordinea Primăriei Țibirica cu statut de persoană juridică. 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 situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informațiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

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

6.1. Măsurile generale de administrare a securităţii informaţionale:

6.1.1. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronic, care conţin date preluate din sistemul resurse umane, aceştia se păstrează în safeuri care se încuie.

6.1.2. La terminarea sesiunilor de lucru, computerul şi imprimanta se deconectează de la reţeaua electrică.

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

6.1.4. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din domeniul resurse umane este blocat împotriva vizualizării de către persoane neautorizate.

6.1.5. Mijloacele de prelucrare a informațiilor preluate din domeniul resurse umane sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

6.1.6. Scoaterea şi introducerea mijloacelor de prelucrare a informațiilor din sistemul resurse umane din/în perimetrul de securitate se înregistrează în Registru.

6.2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul resurse umane, se înfăptuiesc ţinând cont de necesitatea asigurării confidenţialităţii şi integrității acestora, prin protecţie în formă manuală.

6.3. Accesul în biroul unde este amplasat sistemul resurse umane este restricţionat, fiind permis doar persoanei care are autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi cheia de la lacătul mecanic.

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

6.5. Înainte de acordarea accesului fizic la sistemul resurse umane, se verifică competențele de acces.

6.6. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul resurse umane, fiind integru din punct de vedere fizic.

6.7. Zilnic, se inspectează perimetrul de securitate al clădirii şi al biroului, unde este amplasat sistemul resurse umane, din punct de vedere fizic.

6.8. Computerul este amplasat în locuri cu acces limitat pentru persoane străine.

6.9. Uşile şi ferestrele sunt încuiate în cazul în care în încăpere lipsește angajatul autorizat de administrarea sistemului.

6.10. Amplasarea sistemului resurse umane răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

6.11. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului resurse umane, 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 resurse umane, inclusiv posibilitatea deconectării oricărui component TI.

6.12. Computerul, unde este amplasat fizic sistemul resurse umane, dispune de UPS, care este folosit pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

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

6.14. Securitatea antiincendiară a sistemului resurse umane: biroul unde este amplasat sistemul resurse umane este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiare în vigoare.

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 resurse umane. 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 SISTEMELE DE EVIDENȚĂ RESURSE UMANE

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

7.2. Se efectuează înregistrările de audit a securității registrelor ținute manual în care sunt prelucrate date cu caracter personal, conform următorilor parametri:

- 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 resurse umane (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 resurse umane 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.

VIII. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI RESURSE UMANE

8.1. Persoanele care asigură exploatarea sistemului resurse umane 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, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul resurse umane.

8.3. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din sistemul resurse umane poartă răspundere civilă, contravenţională şi penală.

8.4. În cazul producerii incidentelor de securitate în cadrul Primăriei Ţibirica, persoana resposabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova.

8.5. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă resurse umane, care conţin date cu caracter personal, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

IX. DISPOZIŢII FINALE

9.1. Prezentul Regulament este periodic revizuit cu aprobarea modificărilor intervenite în acesta de către Consiliul local Ţibirica.

9.2. Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

9.3. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.

9.4. Prezentul Regulament va fi adus la cunoştinţa angajaţilor Primăriei Ţibirica şi tuturor subdiviziunilor acesteia, contra semnătură.

Secretar al consiliului comunal Ţibirica **FĂRÎMĂ Ala**

ANEXA nr.4
la Decizia Consiliului Local
nr. 08/14 din 09 decembrie 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 Consiliului local a prevederilor Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, Legii contabilității nr. 113 din 27 aprilie 2007 şi a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14 decembrie 2010, precum şi 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 Primăriei Țibirica 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;
- sexul;
- data nașterii și locul nașterii;
- semnătura;
- numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);
- cetățenia;
- semnătură digitală;
- date din actele de stare civilă;
- date din certificatul de înmatriculare;
- codul asigurării medicale (CPAM);
- telefon fix/mobil/fax;
- e-mail;
- profesie, funcție deținută;
- formarea profesională (diplome, studii);
- situație familială;
- datele pentru transferul pe contul bancar a plăților salariale și a altor sume datorate cu titlu de indemnizații, compensații sau alte beneficii, după caz;
- 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;
- imagine;
- date din permisul de conducere;
- sancțiuni disciplinare;
- codul personal de asigurări sociale (CPAS);
- adresa (domiciliul/reședința);
- loc de muncă;
- numărul personal de identificare de stat (IDNP);

- situație militară;
- mărimea salariului brut și alte premii, sporuri, stimulări, suplimente;
- datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare.

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 Primăriei Țibirica și care au impact asupra calculării plăților salariale, precum și a persoanelor fizice și juridice cu care Primăria Țibirica intră în relații contractuale;

b) Calcularea drepturilor salariale lunare, în conformitate cu legislația în vigoare a Republicii Moldova (conform contractelor individuale de muncă, tabelelor de pontaj, ordinelor și 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 (IPC18, IRM 19) și rapoartelor trimestriale privind primele de asigurare obligatorie de asistență medicală (Formularul MED08, M1);

h) 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;

i) Completarea lunară, trimestrială și anuală a dărilor de seamă cu prezentarea acestora Inspectoratului Fiscal de Stat (privind impozitul pe venit IRV 14, TFD 13, IALS 14, MED 08), precum și perfectarea și eliberarea informației privind veniturile calculate și achitate în folosul persoanei fizice și impozitul pe venit reținut din aceste venituri angajaților Primăriei Țibirica;

j) 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;

k) Eliberarea certificatelor de salariu, la cererea angajaților;

l) 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);

m) Emiterea, transmiterea si primirea documentelor financiar-contabile (facturi, anexe la facturi, documente justificative, acte de prestare servicii);

n) Prezentarea documentelor financiare ce conțin date cu caracter personal către acționari/fondatori, comisiei de cenzori, auditului intern sau extern. În cazul datelor cu caracter personal ale angajaților sau ale altor persoane cu care Primăria Țibirica se află în relație juridică, îi va înștiința pe acești atunci când datele respective vor fi transmise către terți.

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 sunt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămâne la păstrare primind statut de document de arhivă.

2.5. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență contabilă în alte scopuri decât 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 cadru Primăriei Țibirica, raionul Călărași se prelucrează/stochează:

- pe suport de hârtie;
- în format electronic:

a) Software – Sistemul de evidență contabilă 1C, versiunea V 8-500 care este instalat la computerul central – "Contabil Șef" și cu drept de acces la al doilea computer – "Materiale", computerele aflându-se în contabilitatea Primăriei Țibirica;

b) Hardware – calculator nr. de inventariere 314.60001 și 314.60039.

3.2. Mentenanța programului contabil 1C este efectuată de către compania fiind încheiat anual contract de valoare mică privind prestarea serviciilor de deservire între Primăria Țibirica și compania 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 Primăriei Țibirica
- Examinarea bazei de date a Primăriei Țibirica (la necesitate);
- Vizite la fața locului, la solicitarea Primăriei Țibirica;
- 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 hârtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri, care sunt amplasate fizic în contabilitatea Primăriei Țibirica.

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 primăriei Țibirica din momentul semnării contractului până 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 sunt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul dosarelor din Primăriei, aprobat de primarul comunei Țibirica la 26.11.2018, ulterior fiind supuse distrugerii sau ștergerii, în funcție de suportul pe care au fost efectuate.

V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE:

5.1. Primăria Țibirica, 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 primarului comunei Țibirica. 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 şi alte persoane şi nu există posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

VI. MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENŢĂ CONTABILĂ:

6.1. Măsurile generale de administrare a securităţii informaţionale:

6.1.1. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronic care conţin date preluate din sistemul de evidenţă contabilă, aceştia se păstrează în safeuri care se încuie.

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

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

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

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

6.1.6. Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidenţă contabilă din/în perimetrul de securitate se înregistrează în Registru.

6.2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidenţă contabilă, se înfăptuiesc ţinând cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică.

6.3. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă contabilă, care conţin date cu caracter personal, sunt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

6.4. Accesul în biroul unde este amplasat sistemul de evidenţă contabilă este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi cheia de la lacătul mecanic.

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

6.6. Înainte de acordarea accesului fizic la sistemul de evidenţă contabilă, se verifică competenţele de acces.

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

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

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

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

6.11. Uşile şi ferestrele sunt încuiate în cazul în care în încăpere lipsesc angajaţii autorizaţi de administrarea sistemului.

6.12. Amplasarea sistemului de evidenţă contabilă răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

6.13. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă contabilă, a cablurilor electrice,

inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele de evidenţă contabilă, inclusiv posibilitatea deconectării oricărui component TI.

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

6.15. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă contabilă, sunt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaţionale.

6.16. Securitatea antiincendiară a sistemului de evidenţă contabilă: biroul unde este amplasat sistemul de evidenţă contabilă este dotat cu echipament antiincendiar şi corespunde cerinţelor şi normelor antiincendiare în vigoare.

6.17. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidenţă contabilă. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

VII. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENŢĂ CONTABILĂ:

7.1. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemele de evidenţă contabilă şi a proceselor executate în numele acestor utilizatori.

7.2. Toţi utilizatorii (inclusiv personalul care asigură mentenanţa tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

7.3. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lângă cerinţele de păstrare a confidenţialităţii parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepţia cazului de asigurare a securităţii păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

7.4. Se efectuează modificarea parolelor de fiecare dată când sunt depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.

7.5. Întru asigurarea posibilităţii de stabilire a responsabilităţii fiecărui utilizator, sunt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. După trei tentative greşite 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 şi prevenirea folosirii repetate a acestora.

7.7. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizaţii de acces primite în scopul comiterii unei fapte prejudiciabile, absenţă a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi 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 evidenţă contabilă, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea 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 şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

7.9. În scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidenţă contabilă.

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

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

a) să vizualizeze informațiile stocate în sistemul de evidență contabilă;

b) să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

7.12. Toţi angajaţii cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor cu caracter personal.

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

7.14. Orice încălcare a securităţii în ceea ce priveşte 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 sunt informaţi despre faptul că folosirea sistemului de evidență contabilă este controlată şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia civilă, contravenţională şi penală.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE DE EVIDENŢĂ CONTABILĂ:

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

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

a) data şi timpul tentativei intrării/ieşirii;

b) ID-ul utilizatorului;

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

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

a) data şi 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 obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informațiilor din sistemul de evidență contabilă, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);

b) denumirea (identificatorul) aplicaţiei sau a procesului;

c) ID-ul utilizatorului;

d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);

e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);

f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

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

a) data şi timpul modificării competenţelor;

b) ID-ul administratorului care a efectuat modificările;

c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

8.6. Se efectuează înregistrarea ieşirii din sistemul de evidenţă contabilă, înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

a) data şi timpul eliberării;

b) denumirea informaţiei şi căile de acces la aceasta;

c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);

d) ID-ul utilizatorului care a solicitat informaţia;

e) volumul documentului eliberat (numărul paginilor, filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

8.7. Cazurile de deranjament al auditului securităţii în sistemul de evidenţă contabilă sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sunt aduse la cunoştinţa persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

8.8. Rezultatele auditului securităţii în sistemul de evidenţă contabilă (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.

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

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIILOR DIN SISTEMUL DE EVIDENŢĂ CONTABILĂ :

9.1. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor din sistemul de evidenţă contabilă, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

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

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

9.4. Copiile de siguranţă: reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranţă a informaţiilor din sistemul de evidenţă contabilă şi soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENŢĂ CONTABILĂ:

10.1. Persoanele care asigură exploatarea sistemului de evidență contabilă trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

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

10.3. În cazul producerii incidentelor de securitate persoanele responsabile vor întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, vor efectua analiza acestuia şi vor 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 sunt 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 obţinerea, păstrarea, prelucrarea şi protecţia informațiilor din sistemul de evidență contabilă poartă răspundere civilă, contravențională și penală.

10.5. Cerințe speciale față de marcare: toate informațiile ieşite din sistemul de evidență contabilă, care conţin date cu caracter personal, sunt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

XI. DISPOZIŢII FINALE:

11.1. Prezentul Regulament este periodic revizuit, cu aprobarea modifiărilor intervenite în acesta de către Consiliul comunal Ţibirica.

11.2. Prezentul Regulamentul se complectează cu prevederile legislației în vigoare.

11.3. Modificarea şi completarea Regulamentului se face în modul stabilit pentru aprobarea lui.

Secretarul Consiliului comunal Ţibirica **FĂRÎMĂ Ala**