REPUBLICA MOLDOVA
CONSILIUL ORĂȘENESC REZINA
raionul Rezina

РЕСПУБЛИКА МОЛДОВА
ГОРОДСКОЙ СОВЕТ РЕЗИНА
Резинского района

DECIZIE nr. 5/18
din 30 august 2024
orașul Rezina

„Cu privire la aprobarea unor acte privind asigurarea protecției datelor cu caracter personal la prelucrarea acestora (scopul și mijloacele de prelucrare a datelor)".

În scopul asigurării protecției datelor cu caracter personal, în temeiul art.14 alin.(3) din Legea nr.436/2006 privind administrația publică locală, Legii nr.133/2011 privind protecția datelor, Legii nr.148/2023 privind accesul la informațiile de interes public, Codului administrativ nr.116/2018, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, consiliul orășenesc Rezina, raionul Rezina,

DECIDE:

1. Se aprobă Cerințele privind asigurarea securității datelor cu caracter personal și prelucrarea acestora în cadrul primăriei orașului Rezina și instituțiile din subordine, (anexa nr.1).
2. Se aprobă Regulamentul privind supravegherea prin mijloace video în cadrul primăriei orașului Rezina, (anexa nr.2) .
3. Se aprobă Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență și examinare a corespondenței și petițiilor parvenite în adresa primăriei orașului Rezina, (anexa nr.3).
4. Se aprobă Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă a primăriei orașului Rezina, (anexa nr.4).
5. Se aprobă Regulamentul cu privire la asigurarea securității datelor cu caracter personal în sistemul de evidență a resurselor umane în cadrul primăriei orașului Rezina și instituțiile din subordine, (anexa nr.5).
6. Primarul orașului Rezina în colaborare cu specialiștii din cadrul primăriei va asigura executarea prezentei deciziei.
7. Prezenta decizie urmează a fi adusă la cunoștință publică, se publică pe site-ul www.actelocale.gov.md și poate fi contestată în decurs de 30 de zile cu respectarea procedurii prealabile la consiliul orășenesc Rezina.

Au votat: pentru – 19; contra – 0 ; s-au abținut – 0.

Președinte al ședinței — Mihail Doni

Secretara consiliului orășenesc — Lilia Răileanu

Anexa nr.1
la decizia consiliului orășenesc Rezina nr.5/18 din 30 august 2024

CERINȚE
privind asigurarea securității datelor cu caracter personal și prelucrarea acestora în cadrul primăriei orașului Rezina și instituțiile din subordine.

I.PREAMBUL. La prelucrarea datelor cu caracter personal în cadrul instituțiilor 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 celor 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 și alte acte legislative/normative de profil.

II. NOȚIUNI GENERALE În prezentul Regulament, sînt 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 teritoriale, 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;

Fișiere temporare – ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat pînă 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 și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;

Mijloace de protecție criptografică a informației care conține date cu caracter personal – mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicații;

Nivel de protecție – nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor,

elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri;

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

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

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

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

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

Restaurarea datelor – procedurile cu privire la reconstituirea/prestabilirea datelor cu caracter personal în starea în care se aflau pînă 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 pînă la momentul opririi acestora;

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

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;

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

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

III. *OBIECTIVELE POLITICII DE SECURITATE*

1. Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de primăria oraşului şi instituţiile din subordine, atît în cadrul prelucrării manuale, cît şi sistemelor şi proceselor de tehnologie informaţională. Securitatea reprezintă o componentă esenţială a derulării optime a proceselor bazate pe IT. Baza unei securităţi IT adecvate o constituie respectarea acestor reguli. 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. Avînd 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 oraşului şi instituţiile din subordine vor proteja datele cu caracter personal atît a petiţionarilor/vizitatorilor, cît şi a angajaţilor săi.

2. Reglementările prezentului regulament reprezintă un standard minim pentru primăria oraşului Rezina, inclusiv toţi angajaţii primăriei şi instituţiilor din subordine.

3. Pornind de la această reglementare, toţi angajaţii primăriei oraşului şi instituţiilor din subordine urmează să respecte strict prevederile Regulamentului şi regulilor interne privind protecţia datelor cu caracter personal şi sistemelor IT.

IV. *DISPOZIŢII PRIVIND IERARHIA ŞI RESPONSABILITATEA PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE*

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

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

6. 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 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 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 încît să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date, va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

V. *MIJLOACE SUPUSE PRINCIPIILOR DE PROTECTIE A DATELOR CU CARACTERE PERSONAL*

7. Protecţia datelor cu caracter personal în cadrul primăriei oraşului Rezina (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice şi

organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal. Sînt supuse protecţiei prin mijloace/procedee specifice, toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin date cu caracter personal, păstrate pe: 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.

VI. MĂSURILE DE PROTECŢIE A DATELLOR CU CARACTER PERSONAL

8. Măsurile de protecţie a datelor cu caracter personal sunt asigurate în scopul: preîntîmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta; preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale; neadmiterea dezvăluirii terţilor a informaţiei cu accesibilitate limitată; eficientizarea resurselor informaţionale atît pe suport de hîrtie cît şi cel în format electronic.

VII. METODE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAŢIONALE

9. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode: preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele,excluderea accesului neautorizat la datele cu caracter personal prelucrate; preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program; preîntîmpinarea 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, preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, preîntîmpinarea 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, preîntîmpinarea 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 informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenţă instituite atît pentru utilizatorii interni cît şi pentru cei externi.

VIII. PROCEDURI ORGANIZATORICE ŞI TEHNICE

10. Procedurile organizatorice şi tehnice care urmează a fi respectate la prelucrarea datelor cu caracter personal sunt de ordin administrativ şi tehnologic precum este menţionat mai jos: 1. Măsurile generale de administrare a securităţii informaţionale: a) în cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie, b) computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru, c) este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copier, d) este asigurată securitatea şi accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate, e) mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii, f) Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere, g) este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

11. Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal: a) accesul în sediile/oficiile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare), b) se asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces, c) perimetrul de securitate a primăriei reprezintă perimetrul sediului în care se prelucrează/stochează date cu caracter personal, d) perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sînt rezistenţi, intrările sunt echipate cu lacăte şi semnalizare, e) amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri, f) uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc membrii, g) computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine, h) accesul în perimetrul de securitate a clădirii primăriei unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ţinînd cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 şi art. 30 ale Legii privind protecţia datelor cu caracter personal, precum şi pct. 26 din Cerinţe, i) folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii.

12. 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 sînt 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.

13. 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.

14. Administrarea identificatorilor utilizatorilor include: identificarea univocă a fiecărui utilizator, verificarea autenticităţii fiecărui utilizator.

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

15. Controlul administrării acţiunilor utilizatorilor este efectuat sistematic în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Accesul de la distanţă: a) Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi

sînt documentate, supuse monitorizării şi controlului, b) fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este autorizată de persoanele responsabile ale primăriei şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

16. 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.

17. 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 sînt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

18. 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, evitîndu-se folosirea funcţiilor standarde de nimicire.

19. Dezvăluirea datelor cu caracter personal: a) dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informaţii sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN.

20. 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.

21. 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, înmînarea personală, etc.). Dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund Cerinţelor, (spre exemplu: expedierea informaţiei prin intermediul e-mailurilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.) sînt interzise. Sînt interzise operaţiunile de dezvăluire a datelor cu caracter personal între primărie şi alte entităţi care sunt amplasate geografic în stînga Nistrului care refuză să se supună juridic legislaţiei Republicii Moldova, reieşind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce ţine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecţia datelor cu caracter personal. Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie şi/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituţional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecţie a datelor cu caracter personal. Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecţia datelor cu caracter personal, în special în cazurile cînd tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

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

23. Acces la sistemele informaţionale gestionate în cadrul primăriei, din partea Procuraturii Generale (după caz procuraturile teritoriale/specializate), Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi art. 212 Cod de procedură penală. Se explică că în conformitate cu prevederile art.157 Cod de procedură penală, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adeverite circumstanţe care au importanţă pentru cauză, (inclusiv informaţia stocată în auditul sistemelor informaţionale şi de evidenţă), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate şi răspîndite fără necesitate informaţie oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată (inclusiv operatorii de date cu caracter personal) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date.

24. 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 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. 741 Cod contravenţional.

25. Drepturile subiecţilor de date cu caracter personal: a) în cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecţia datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informaţii, exceptînd cazul în care el deţine deja informaţiile respective: - privind identitatea operatorului, a persoanei împuternicite de către operator, sau, după caz, a reprezentantului operatorului (denumirea, adresa juridică, IDNO-ul); - datele de contact ale responsabilului de protecţia datelor personale, după caz; - privind scopul concret al prelucrării datelor cu caracter personal colectate; - privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal; - existenţa drepturilor la informare şi de acces la datele colectate; de intervenţie asupra datelor (în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia.

26. Subiecţilor de date cu caracter personal le este asigurat dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţi subiecţi, conţinute în fişele personale (alte materiale), cu excepţia cazurilor în care solicitanţii îşi realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

27. 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.

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 urmînd a fi efectuată în toate sistemele informaționale și de evidență gestionate.

28. Accesul în spațiile/perimetrul unde sînt 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 instituționale /regulamentelor departamentale aprobate.

29. Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sînt conectate la internet, nu sînt 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.

30. 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 sînt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul primăriei.

31. Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie 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.

32. Auditul sistemelor informaționale gestionate: 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 negative; 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.

33. 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.

Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri: data și timpul eliberării, denumirea informației și căile de acces la aceasta, - specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic), ID-ul utilizatorului, care a solicitat informația.

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

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

34. 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.

Personalul primăriei informează neîntîrziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

35. Pînă la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrul Naţional pentru Protecţia Datelor cu Caracter Personal despre incidentele de securitate constatate. În cazul producerii incidentelor de securitate în cadrul primăriei 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.

În cadrul controalelor efectuate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar şi asigurat accesul la informaţiile necesare relevante obiectului controlului.

36. Toată informaţia care se intenţionează a fi dezvăluită, şi care conţine date cu caracter personal, urmează a fi marcată prin: Model - Atenţie! Documentul conţine date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal

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

38. Primăria oraşului Rezina va aduce la cunoştinţa angajaţilor prezentele cerinţe privind securitatea datelor cu caracter personal din cadrul primăriei oraşului Rezina şi instituţiile din subordine.

Secretara consiliului orăşenesc Rezina Lilia Răileanu

Anexa nr.2
la decizia consiliului orășenesc Rezina nr.5/18 din 30 august 2024

Regulament
privind supravegherea prin mijloace video în cadrul primăriei orașului Rezina

Dispoziții generale

1. În contextul actual securitatea obiectivelor nu poate fi asigurată fără o supraveghere video eficientă, care să permită, atît monitorizarea în timp real a evenimentelor și persoanelor suspecte, cît și înregistrarea imaginilor video a spațiilor publice din teritoriul administrat cît și birourilor de acces public din incinta primăriei orașului Rezina.

Totodată utilizarea unui astfel de sistem include anumite responsabilități și garanții din partea proprietarului de sistem, referitor la prelucrarea și protecția datelor cu caracter personal ce se înregistrează în sistem, atribuții și reglementări descrise în Legea nr. 133/2011 privind protecția datelor cu caracter personal.

Din acest motiv este necesară stabilirea unui regulament de securitate privind supravegherea prin mijloace video și prelucrarea datelor cu caracter personal preluate și înregistrate în sistemul de supraveghere prin mijloace video.

Mijloacele de supraveghere video se instalează și utilizează cu respectarea principiului:

a) legalității;

b) proporționalității;

c) transparenței;

d) securității.

2. Regulamentul privind supravegherea prin mijloace video în cadrul primăriei orașului Rezina are drept scop:

- Stabilirea unui set unitar de reguli care reglementează implementarea și utilizarea sistemului de supraveghere prin mijloace video, în scopul asigurării securității persoanelor, pazei și protecției bunurilor, imobilelor, valorilor și a materialelor cu regim special, respectînd în același timp obligațiile ce revin entității, în calitate de operator de date, conform Legii nr. 133/2011 și măsurile de securitate adoptate pentru protecția datelor cu caracter personal, protejarea vieții private, a intereselor legitime și garantarea drepturilor fundamentale ale persoanelor vizate.
- Stabilirea responsabilităților privind administrarea și exploatarea sistemului de supraveghere prin mijloace video, precum și cele privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.
- Scopul utilizării sistemului de supraveghere prin mijloace video este de a asigura buna administrare și funcționare a entității, în special în vederea controlului de securitate și pază. De asemenea, sistemul de supraveghere prin mijloace video este necesar pentru a sprijini politicile de securitate instituite de actele normative care reglementează protecția datelor cu caracter personal și contribuie la îndeplinirea atribuțiilor structurii de securitate.

Prezentul Regulamentul descrie măsurile care necesită a fi luate de primăria orașului Rezina pentru a proteja datele cu caracter personal care sînt prelucrate prin metoda supravegherii video, vieții private și alte drepturi fundamentale și interese legitime ale subiecților.

3. Zonele supravegheate

- Camerele de supraveghere video sînt amplasate în locuri vizibile. Orice utilizare ascunsă a acestora este strict interzisă, cu excepția cazurilor expres reglementate de legislație.
- Camerele de supraveghere video sînt amplasate conform schemei de amplasare coordonată cu persoanele interesate.

Nu sînt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum birourile de serviciu şi toaletele. Instalarea mijloacelor de supraveghere video se poate realiza numai în condiţiile în care echipamentele sînt orientate exclusiv asupra căilor de acces şi perimetrului acestor bunuri, fără ca în raza lor de acoperire să fie vizualizate bunurile terţilor.

4. Datele cu caracter personal colectate prin intermediul sistemului de supraveghere prin mijloace video.

- Sistemul de supraveghere prin mijloace video este dotat parţial cu cu detector de mişcare.
- Toate camerele funcţionează în regim 24/24 ore şi sînt fixate.
- La darea în exploatare a sistemului de supraveghere video, persoana împuternicită va primi instructajul referitor la setările sistemului de supraveghere prin mijloace video, respectarea regimului de confidenţialitate şi dreptul de acces la informaţia prelucrată în sistemul de evidenţă.

5. Limitarea scopului

- Sistemul de supraveghere prin mijloace video va fi utilizat numai în scop legal, fără a se urmări în special obţinerea unor informaţii pentru anchetele interne sau procedurile disciplinare, cu excepţia situaţiilor în care se produce un incident de securitate sau se observă un comportament infracţional (în circumstanţe excepţionale imaginile pot fi transmise organelor competente în cadrul unor investigaţii disciplinare sau penale).
- În vederea protejării vieţii private a altor subiecţi decît cei vizaţi nemijlocit, sistemul de supraveghere prin mijloace video este dotat cu mecanisme care prevăd estomparea imaginii (în caz de necesitate) pentru a face ca întreaga imagine sau o parte a ei, după caz, să fie anonimizată.
- Persoana responsabilă va gestiona accesul la sistemul de supraveghere prin mijloace video numai cu acordul scris al conducerii primăriei oraşului Rezina (primar, viceprimar, secretarul consiliului orăşenesc).

6. Categorii speciale de date cu caracter personal

- Sistemul de supraveghere prin mijloace video al primăriei oraşului Rezina nu are ca scop captarea (spre exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (spre exemplu indexare, creare de profiluri) care constituie categoria specială de date cu caracter personal.

7. Accesul la datele cu caracter personal şi dezvăluirea acestora

- Accesul la imaginile video înregistrate în timp real este limitat la un număr redus de angajaţi ai primăriei oraşului Rezina, care pot fi identificaţi individual, în conformitate cu lista aprobată de către primarul oraşului Rezina.
- Accesul la imaginile video şi/ sau la arhiva în care sînt stocate imaginile înregistrate este permis numai persoanei responsabile în conformitate cu Politica de securitate a primăriei oraşului Rezina şi numai cu acordul scris al conducerii.
- Vizualizarea şi/sau efectuarea copiilor din fişierele temporare în care sînt stocate imaginile video, este permis numai cu acordul scris al conducerii.
- În cazul solicitării de către organele de drept ale Republicii Moldova, care îşi exercită atribuţiile conform legii, a unor copii din fişierele temporare în care sînt stocate imaginile video, este permis numai cu acordul scris al conducerii primăriei oraşului Rezina.

8. Protecţia sistemului informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video.

- Sistemul video este autonom şi nu este conectat la reţeaua internet.
- În vederea securizării sistemului informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video, se aplică următoarele măsuri tehnice şi organizatorice:
- sistemul informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video se păstrează în camera special amenajată din incinta clădirii primăriei;
- responsabilul de protecţie a datelor cu caracter personal şi responsabilii de Securitate din cadrul primăriei vor fi consultaţi înainte de achiziţionarea sau instalarea oricărui nou sistem de supraveghere prin mijloace video;
- toate sistemele trebuie să corespundă cerinţelor de securitate descrise în legislaţie (vezi Hotărîrea Guvernului nr.1123/2010 privind aprobarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal);

- accesul fizic la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video are numai persoana responsabilă desemnată de primarul orașului;
- accesul la înregistrările video prelucrate este restricționat prin introducerea unui șir de parole;
- în cazul deconectării energiei electrice, sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu sursă autonomă de alimentare cu energie electrică (UPS);
- sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu firewall care asigură protecția în rețea.

Echipamentele sînt astfel instalate încît să se afle sub supraveghere doar acele spații identificate în analiza de risc ca avînd nevoie de protecție suplimentară. Utilizatorii sistemului de supraveghere prin mijloace video sunt instruiți să nu monitorizeze astfel de zone.

9. Control Acces

- Imaginile captate de sistemul de supraveghere prin mijloace video sînt vizualizate în timp real pe monitoarele din camera de control acces, care reprezintă o încăpere securizată, iar monitoarele nu pot fi văzute din exterior. Camera de control acces este amplasată în sediul primăriei.
- Accesul neautorizat în Camera de control este interzis. Accesul este permis la angajații autorizați: personalul cu funcții de asigurare al securității fizice și control acces, administratorul de sistem, responsabilii cu securitatea informației și conducerea entității.
- De la caz la caz, se poate acorda accesul în Camera de control și altor persoane, în afara celor menționate mai sus, doar pe bază de autorizare din partea responsabilului de securitate din cadrul entității. Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video, accesul acestora fiind permis strict pentru executarea lucrărilor menționate în autorizarea din partea responsabilului de securitate din cadrul entității.

10. Măsuri tehnice și organizatorice

Pentru a proteja securitatea sistemului de supraveghere prin mijloace video și pentru a spori gradul de protecție a vieții private, au fost introduse următoarele măsuri tehnice și organizatorice:
- limitarea timpului de stocare a materialului filmat, în conformitate cu cerințele de securitate și legislația în vigoare privind conservarea datelor;
- mediile de stocare (serverele pe care se stochează imaginile înregistrate) se află în spații securizate și protejate de măsuri de securitate fizică;
- toți utilizatorii cu drept de acces la sistemul de supraveghere prin mijloace video au semnat acorduri de confidențialitate, prin care se obligă să respecte prevederile legale în domeniu;
- utilizatorilor se acordă dreptul de acces doar pentru acele resurse care sînt strict necesare pentru îndeplinirea atribuțiilor de serviciu;
- doar administratorii de sistem numiți în acest sens de către operator, și responsabilul de securitate, au dreptul de a accesa fișierele înregistrate în sistem, la cererea conducerii primăriei.

11. Drepturi de acces

Accesul la imaginile stocate și/sau la arhitectura tehnică a sistemului de supraveghere prin mijloace video este limitat la un număr redus de persoane și este determinat prin atribuțiile specificate, în care este indicat în ce scop și ce tip de acces este acordat.

Primăria orașului Rezina impune limite stricte în privința persoanelor care au dreptul:
- să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile responsabililor de securitate și agenților de pază desemnați să desfășoare activitatea de supraveghere;
- să vizioneze înregistrarea materialului filmat: vizionarea imaginilor înregistrate se va face în cazuri justificate, cum ar fi cazurile prevăzute expres de lege și incidentele de securitate, de către persoanele special desemnate;
- să copieze, să descarce, să șteargă sau să modifice orice material filmat de sistemul de supraveghere prin mijloace video.

12. Instructaj

- Toți membrii personalului cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor.

- Această procedură va fi integrată în programul de instruire şi îndrumare, pentru toţi utilizatorii cu drept de acces şi atribuţii în operarea sistemului de supraveghere prin mijloace video.

13. Măsuri de păstrare a confidenţialităţii. Imediat după instructaj, fiecare participant cu drept de acces la sistemul de supraveghere prin mijloace video semnează un acord de confidenţialitate.

14. Dezvăluirea datelor cu caracter personal

- Orice activitate de dezvăluire a datelor personale către terţi va fi documentată şi supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, şi pe de altă parte compatibilitatea dintre scopul în care se face comunicarea şi scopul în care aceste date au fost colectate iniţial pentru prelucrare.
- Orice situaţie de dezvăluire va fi consemnată de administratorul sistemului într-un Registru de evidenţă a cazurilor de dezvăluire.

Primăria oraşului Rezina are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, înregistrările video în care este surprinsă săvârşirea unor fapte de natură contravenţională/penală.

Sistemul de supraveghere prin mijloace video nu este utilizat pentru verificarea prezenţei la program sau evaluarea performanţei la locul de muncă.

În cazuri excepţionale, dar cu respectarea garanţiilor descrise mai sus, se poate acorda acces altor servicii din cadrul entităţii (Protecţie Antiincendiară, Resurse Umane, Riscuri), în cadrul unei anchete disciplinare, de accidentare sau de securitate, cu condiţia ca informaţiile să ajute la investigarea unei infracţiuni, accident de muncă sau a unei abateri disciplinare de natură să prejudicieze drepturile şi libertăţile unei persoane fizice sau juridice.

15. Durata păstrării înregistrărilor video

- Durata păstrării înregistrărilor video este de 30 zile calendaristice, după care acestea se nimicesc automat în ordinea în care au fost înregistrate.
- În cazul producerii unui incident de securitate, durata de păstrare a înregistrărilor video poate depăşi limitele admisibile de program, în funcţie de timpul necesar investigării suplimentare a incidentului de securitate.

16. Informarea publicului referitor la supravegherea video. Informarea publicului referitor la supravegherea video din teritoriul administrat se efectuează prin pictograme. Primăria garantează că asigură respectarea drepturilor ce revin persoanelor vizate, în conformitate cu legislaţia Republicii Moldova. Toate persoanele implicate în activitatea de supraveghere video şi cele responsabile de administrarea imaginilor filmate, vor respecta procedurile şi regulamentele de acces la date cu caracter personal ale entităţii.

17. Informarea persoanelor vizate. Informarea primară a persoanelor vizate se realizează în mod clar şi permanent, prin intermediul unui semn adecvat, cu vizibilitate suficientă şi localizat în zona supravegheată, astfel încît să semnaleze existenţa camerelor de supraveghere, dar şi pentru a comunica informaţiile esenţiale privind prelucrarea datelor cu caracter personal.

Persoanele vizate sunt atenţionate asupra existenţei sistemului de supraveghere prin mijloace video şi a proprietarului prin note de informare corespunzătoare, care cuprind scopul prelucrării şi identifică primăria oraşului Rezina ca operator al datelor colectate prin intermediul supravegherii video.

18. Exercitarea drepturilor de acces, intervenţie şi opoziţie. Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc deţinute de primăria oraşului , de a solicita intervenţia (ştergere/ actualizare/rectificare/ anonimizare) sau de a se opune prelucrărilor, conform legii. Orice cerere de a accesa, rectifica, bloca şi/sau şterge date cu caracter personal ca urmare a utilizării camerelor video ar trebui să fie adresată direct primăriei oraşului Rezina. În cazul în care persoana vizată are alte întrebări privind prelucrarea de către primăria oraşului a datelor personale care o privesc, se poate adresa conducerii primăriei.

Răspunsul la solicitarea de acces, intervenţie sau opoziţie se dă în termen de 15 zilecalendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra

motivului de amînare a răspunsului, de asemenea i se va comunica şi procedura care va urma pentru soluţionarea cererii.

Dacă există solicitarea expresă a persoanei vizate, se poate acorda dreptul de a vizualiza imaginile înregistrate care o privesc sau i se poate trimite o copie a acestora. Imaginile furnizate vor fi clare, în măsura posibilităţii, cu condiţia de a nu prejudicial drepturile terţilor (persoana vizată va putea vizualiza doar propria imagine, imaginile altor personae care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoaşterea/identificarea lor). În cazul unei asemenea solicitări, persoana vizată este obligată:

- să se identifice dincolo de orice suspiciune (să prezinte actul de identitate cînd participă la vizionare), să menţioneze data, ora, locaţia şi împrejurările în care a fost înregistrată de camerele de supraveghere;
- de asemenea, persoana vizată va prezenta şi o fotografie recentă astfel încît utilizatorii desemnaţi să o poată identifica mai usor în imaginile filmate;
- persoana va putea vizualiza doar propria imagine, imaginile persoanelor care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoaşterea/identificarea lor.

Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune şi în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu dacă în imagini apar şi alte persoane şi nu există posibilitatea de a obţine consimţămîntul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

19. Auditul securităţii sistemului de supraveghere prin mijloace video

Auditul securităţii sistemului de supraveghere prin mijloace video menţine înscrieri de sistem despre evenimentele produse în activitatea sistemului sau a aplicaţiei, precum şi despre activitatea utilizatorului.

În conjuncţie cu instrumentele şi procedurile respective, auditul securităţii sistemului de supraveghere prin mijloace video permite de a promova mijloace de ajutor pentru a atinge obiective de securitate: evidenţa acţiunilor utilizatorului, definirea şi stabilirea responsabilităţii individuale, reconstrucţia evenimentelor, detectarea intruşilor şi problemelor de identificare a evenimentelor.

Auditul securităţii sistemului de supraveghere prin mijloace video este menit să acorde suport la:

- stabilirea consecutivităţii acţiunilor utilizatorului sau proceselor;
- stabilirea cînd, cine sau ce a stopat funcţionarea normală a sistemului;
- soluţionarea problemei de detectare a intruşilor.

Secretara consiliului orăşenesc Rezina Lilia Răileanu

Anexa nr.3
la decizia consiliului orăşenesc Rezina nr. 5/18 din 30 august 2024

Regulamentul
privind prelucrarea informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă şi examinare a corespondenţei şi petiţiilor parvenite în adresa primăriei oraşului Rezina

I.Dispoziţii generale

1. Regulamentul privind prelucrarea informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă şi examinare a corespondenţei şi petiţiilor parvenite în adresa primăriei oraşului Rezina în continuare Regulament este elaborat în conformitate cu prevederile Codului administrativ nr.116/2018, Legii nr. 71/ 2007 cu privire la registre, Legii nr.133/2011 privind protecţia datelor cu caracter personal, 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, 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 sistemului de evidenţă şi examinare a corespondenţei şi petiţiilor parvenite în adresa primăriei oraşului Rezina, precum şi procedura de înregistrare, securizare, modificare şi radiere a datelor din Registru.

3. Noţiunile utilizate în prezentul Regulament:

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

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

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

Propunere – orice propunere prin intermediul căreia se urmăreşte realizarea de către autoritatea publică a unor acţiuni de interes public;

Registrul de evidenţă a corespondenţei – resursa informaţională specializată (totalitatea informaţiilor ţinute în formă automatizată şi manuală) care asigură evidenţa informaţiei sistematizate, principalul obiectiv al căruia constă în asigurarea evidenţei corespondenţei parvenite în primărie;

Registrator – angajatul primăriei oraşului Rezina împuternicit cu atribuţiile de introducere, modificare, păstrare a informaţiei din Registru.

4. Angajaţii primăriei oraşului Rezina poartă răspundere personală pentru îndeplinirea cerinţelor prezentului Regulament, asigurarea confidenţialităţii, securităţii şi păstrarea în stare corespunzătoare a informaţiei din Registru.

5. Petiţiile anonime, înaintate în adresa primăriei oraşului Rezina, în conformitate cu prevederile art. 76 alin. (1) al Codului administrativ nr. 116 /2018 nu se examinează.

II. Condiţii generale faţă de ţinerea sistemului de evidenţă a corespondenţei şi petiţiilor (Registrul)

6. Registrul de evidenţă a corespondenţei şi petiţiilor reprezintă un sistem mixt ce utilizează atât evidenţa în formă electronică, cât şi în formă manuală.

7. De către persoana împuternicită de ţinerea Registrului din cadrul primăriei va fi asigurată ţinerea în formă manuală a unor componente al Registrului (ţinând cont de competenţa funcţională) prin înscrierea informaţiei, inclusiv păstrarea cărţii Registrului, în conformitate cu prevederile legislaţiei în vigoare.

8. Persoana responsabilă din cadrul primăriei va asigura suplimentar evidenţa în formă electronică a corespondenţei şi petiţiilor parvenite la primăria oraşului Rezina.

9. Obiectul înregistrării reprezintă informaţia referitor la persoanele care au depus adresări/petiţii în adresa primăriei oraşului Rezina, consiliului orăşenesc.

10. Registrul va fi ţinut în limba română.

11. Registratorul este obligat:

- să introducă în Registru numai informaţie veridică, colectată de la adresant 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.

12. Datele din registru vor reflecta starea veridică şi actuală a informaţiei privind persoanele care s-au adresat la primăria oraşului Rezina.

13. Atât forma manuală, cât şi cea electronică a Registrului va cuprinde în mod obligatoriu: - denumirea Registrului; - denumirea primăriei oraşului Rezina ca proprietar, 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.

14. 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.

15. Prelucrarea datelor cu caracter personal în sistemul de evidenţă al corespondenţei şi petiţiilor parvenite în adresa primăriei oraşului Rezina se efectuează în conformitate cu prevederilor art. 5 alin. 5 lit. b), d) şi e) al Legii nr.133/2011 privind protecţia datelor cu caracter personal.

III. Condiţii generale privind introducerea informaţiei în Registru

16. Informaţia privind corespondenţa parvenită în adresa primăriei oraşului Rezina va fi recepţionată şi înregistrată în aceiaşi zi de persoana responsabilă din cadrul entităţii şi după caz, în fişele de evidenţă şi control a acestora, iar versiunea electronică parvenită se înregistrează în arhiva electronică a primăriei.

17. Înregistrarea informaţiei în Registru se face prin introducerea menţiunilor necesare în cartea de înregistrări (forma manuală) şi în Sistemul informatic (forma electronică) în baza datelor furnizate prin documentele transmise atât de furnizorul datelor registrului (petiţionarul agentul economic, autoritatea publică), atât pe suport de hârtie sau în formă electronică, perfectate în modul stabilit de lege.

18. La înregistrarea corespondenţei, pe prima pagină se va aplica ştampila de înregistrare în care se indică data primirii şi indicele de înregistrare. Indicele de înregistrare constă după caz, din litera iniţială a numelui şi prenumelui adresantului, numărul şi anul de înregistrare a înscrisului.

19. După caz, se va întocmi manual fişa de evidenţă şi control pentru fiecare adresare (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 Hotărârea 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 oraşului Rezina, termenul de soluţionare stabilit, datele despre starea executării etc.

20. După examinarea şi soluţionarea definitivă, pe fişa de evidenţă şi control se aplică semnătura persoanei responsabile de evidenţă, iar în Sistemul informatic se face menţiunea despre finalizarea acesteia şi modificarea statutului ca „Închis".

21. Modificările şi radierile făcute în Registru se efectuează în baza deciziei şi cu semnătura registratorului în situaţia existenţei unui motiv întemeiat în acest sens.

22. 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.

23. 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.

24. 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.

25. Rectificările şi radierile înscrierilor din Registru se efectuează astfel încât textul iniţial să fie citabil.

IV. Condiţii generale privind păstrarea şi furnizarea informaţiei din Registru

26. Păstrarea Registrului este asigurată de registrator până la adoptarea deciziei conducerii primăriei oraşului Rezina despre lichidarea registrului, dar nu mai mult decât pe perioada stabilită de Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016.

27. Ţinerea Registrului este supusă controlului intern şi extern, în conformitate cu prevederile art. 31 al Legii nr.71/2007 cu privire la registre.

28. 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.

29. Persoanele împuternicite de ţinerea şi controlul registrului sînt obligate să nu divulge informaţia la care au primit acces în legătură cu exercitarea atribuţiilor funcţionale, inclusiv după încetarea activităţii în cadrul primăriei oraşului Rezina.

30. Registratorul este obligat să asigure accesul la informaţia din registru pentru angajaţii autorizaţi ai primăriei oraşului Rezina 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.

31. Informaţia poate fi furnizată gratuit sau contra plată în conformitate cu Legea nr.148/2023 privind accesul la informaţie de interes public.

32. Extrasul din Registru trebuie să fie semnat de conducerea primăriei oraşului Rezina, cu indicarea datei întocmirii/eliberării acestuia.

V. Condiţiile suplimentare privind gestionarea Registrului în forma manuală

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

34. În acest sens, evidenţa corespondenţei în cadrul primăriei oraşului Rezina este dusă prin intermediul mai multor Registre ţinute în formă manuală, cum ar fi: - Registrul petiţiilor e separat de registrul scrisorilor de intrare; - Registru intrări; - Registru ieşiri; - Registru Dispoziţii; - Registrul pentru cereri, sesizări; - Registrul contractelor de muncă; - Registrul contractelor de arendă, locaţiune, vînzare-cumpărare a bunurilor immobile proprietate publică a oraşulu; - Registrul de evidenţă a recruţilor.

35. Registratorul, suplimentar la cele expuse în Cap. IV, în cazul gestionării Registrului în formă manuală, 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 înlocuiască neîntemeiat 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: semnătura şi ştampila.

36. 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; - conţinutul succint al documentului; - numele şi prenumele executantului, termenul de executare şi rezoluţia conducerii primăriei oraşului Rezina; - rezultatul examinării: admisă/respinsă/oferite explicaţii de rigoare/acte de reacţionare adoptate de conducerea primăriei oraşului Rezina - alte date relevante.

37. 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. 79 al Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

VI. Condiţii suplimentare privind gestionarea Registrului în formă electronică

38. Ţinerea în formă electronică a Registrului de evidenţă a corespondenţei este realizat de primăria oraşului Rezina prin intermediul unui sistem informaţional automatizat special constituit - Sistemul informatic.

39. Introducerea, modificarea şi păstrarea informaţiei în acest Registru este asigurată de registratorul desemnat conform fişei postului.

40. La înscrierea informaţiei privind corespondenţa parvenită, în Registru se inserează şi o listă de date despre obiect, inclusiv date cu privire la faptul înregistrării în compartimentele special destinate, şi anume: - tipul adresării; - data şi numărul de intrare; - termenul de rezolvare şi data expirării; - numele, prenumele adresantului; - adresa de domiciliu, e-mail (în cazul existenţei); - numărul de telefon fix/mobil; - conţinutul succint al adresării; - rezoluţia conducerii primăriei oraşului Rezina; - persoana responsabilă de control şi executorul; - copia scanată, în format „.pdf" a adresării; - date privind executarea; - date privind posibila prelungire (termenul, numărul documentul prin care s-a efectuat prelungirea, informarea adresantului; - rezultatul examinării: admisă/respinsă/oferite explicaţii de rigoare/acte de reacţionare adoptate de primăria oraşului Rezina; - alte date relevante privind examinarea corespondenţei şi petiţiilor.

40.1. Sistemul informaţional de evidenţă al corespondenţei şi petiţiilor va fi gestionat, pe toată perioada ciclului de viaţă, în conformitate cu prevederile stabilite de 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. 1123/2010.

VII. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemul de evidenţă a corespondenţei şi petiţiilor

41. La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează.

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

43. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidenţă a corespondenţei şi petiţiilor este blocat împotriva vizualizării de către persoane neautorizate.

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

45. Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidenţă a corespondenţei şi petiţiilor din/în perimetrul de securitate se înregistrează întru-n registru specializat.

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

47. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă a corespondenţei şi petiţiilor, 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. (*Model Atenţie! Documentul conţine date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal).*

48. Accesul în biroul unde este amplasat sistemul de evidenţă a corespondenţei şi petiţiilor 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/sau cheia de la lacătul mecanic.

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

50. Înainte de acordarea accesului fizic la sistemul de evidenţă a corespondenţei şi petiţiilor, se verifică competenţele de acces.

51. 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, conform cerinţelor prevăzute în instrucţiunile cu privire la ţinerea lucrărilor de secretariat.

52. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidenţă a corespondenţei şi petiţiilor, fiind integru din punct de vedere fizic.

53. Zilnic, se inspectează perimetrul de securitate al clădirii şi al biroului, unde este amplasat sistemul de evidenţă a corespondenţei şi petiţiilor, din punct de vedere fizic.

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

55. Uşile şi ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajaţii autorizaţi de administrarea sistemului.

56. Amplasarea sistemului de evidenţă a corespondenţei şi petiţiilor răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

57. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă a corespondenţei şi petiţiilor, 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 registru, inclusiv posibilitatea deconectării oricărui component.

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

VIII. *Identificarea şi autentificarea utilizatorului sistemului de evidenţă a corespondenţei şi petiţiilor*

59. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemul de evidenţă a corespondenţei, petiţiilor şi a proceselor executate în numele acestor utilizatori.

60. Toţi utilizatorii (inclusiv 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.

61. Pentru confirmarea ID-ului utilizatorului sînt 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.

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

63. 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.

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

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

66. Orice încălcare a securităţii în ceea ce priveşte sistemul de evidenţă a corespondenţei şi petiţiilor este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

67. Înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea registrului este controlată şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia civilă, contravenţională şi penală.

IX. Auditul securităţii în sistemul de evidenţă a corespondenţei şi petiţiilor

68. Se organizează generarea înregistrărilor de audit a securităţii în sistemul de evidenţă a corespondenţei şi petiţiilor pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

69. 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;

70. Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informaţiilor din registrul de evidenţă a corespondenţei, conform următorilor parametri: a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii); b) ID-ul utilizatorului; c) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.); d) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.).

71. Cazurile de deranjament al auditului securităţii în sistemul de evidenţă a corespondenţei şi petiţiilor sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt 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.

72. Rezultatele auditului securităţii în sistemul de evidenţă a corespondenţei şi petiţiilor (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.

73. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidenţă a corespondenţei şi petiţiilor 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.

X. Asigurarea integrităţii informaţiilor din sistemul de evidenţă a corespondenţei şi petiţiilor

74. Copiile de siguranţă a informaţiilor din sistemul de evidenţă a corespondenţei, petiţiilor şi soft-urilor folosite pentru prelucrările automatizate a acestora vor fi efectuate în regimul automat, zilnic, reieşind din volumul prelucrărilor efectuate. 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.

XI. Gestionarea incidentelor de securitate a sistemului de evidenţă a corespondenţei şi petiţiilor

75. Persoanele care asigură exploatarea sistemului de evidenţă a corespondenţei şi petiţiilor 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.

76. 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 evidenţă a corespondenţei şi petiţiilor.

77. În cazul producerii incidentelor de securitate persoanele responsabile vor 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. Totodată, în cadrul controalelor efectuate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar şi să asigure accesul la informaţiile necesare relevante obiectului controlului.

78. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din sistemul de evidenţă a corespondenţei şi petiţiilor poartă răspundere civilă, contravenţională şi penală.

XII. Dispoziţii finale

79. Prezentul Regulament este revizuit şi ulterior aprobat de către consiliul orăşenesc periodic, însă cel puţin o dată în an, precum şi la necesitate.

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

81. Regulamentul este adus la cunoştinţa angajaţilor contra semnăturii.

Secretara consiliului orăşenesc Rezina Lilia Răileanu

Anexa nr.4
la decizia consiliului orășenesc Rezina nr. 5/18 din 30 august 2024

REGULAMENTUL

privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă a primăriei orașului Rezina

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 primăriei orașului Rezina, a prevederilor Legii nr.133/2011 privind protecția datelor cu caracter personal, Legii contabilității nr. 113/2007 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.1123/2010, precum și întru respectarea prevederilor art. 91 - 94 ale Codului muncii nr.154/2003.

Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților primăriei orașului Rezina inclusiv din cadrul intituțiilor din subordine 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. Prelucrarea datelor cu caracter personal în sistemul de evidență contabilă se efectuează în conformitate cu prevederile art. 5 alin. 5 lit. a), b) și e) al Legii nr.133/2011 privind protecția datelor cu caracter personal.

2.3. În cadrul sistemului de evidență contabilă sînt prelucrate următoarele categorii de date cu caracter personal: numele, prenumele și patronimicul; sexul; numărul personal de identificare de stat (IDNP); data nașterii și domiciliul; telefon mobil/fix/fax; semnatura/semnatura digitala; date din acte de stare civilă, profesie, funcție, formare profesională, diplome, studii, cetatenia;situatie economica sau financiara; imagine; date bancare, date din permisul de conducere, sancțiuni disciplinare, codul personal de asigurări sociale (CPAS); codul personal de asigurări medicale (CPAM); adresa domiciliului ,reședinței, datele privind locul de muncă, mărimea salariului brut și alte premii, sporuri, stimulări, datele privind situația familială ; datele din certificatele de concediu medical.

2.4. 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 orașului Rezina inclusive din instituțiile din subordine și care au impact asupra calculării plăților salariale, precum și a persoanelor fizice și juridice cu care primăria orașului Rezina intră în relații contractuale; b) Calcularea drepturilor salariale lunare, în conformitate cu legislația în vigoare a Republicii Moldova (conform contractelor individuale de muncă, contractelor civile, tabelelor de pontaj, ordinelor/dispozițiilor conducerii, raportului de activitate lunară); c) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor de incapacitate temporară de muncă; d) Prelucrarea copiilor ordinelor/dispozițiilor conducerii referitoare la personal; e) Calcularea și reținerea taxelor ce țin de plățile salariale aferente angajaților: primele de asigurare obligatorie de asistență medicală, contribuțiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.; f) Calcularea și virarea primelor de asigurare obligatorie de asistență medicală și a contribuțiilor la bugetul asigurărilor sociale de stat, aferente plăților salariale - obligație a angajatorului; g) Furnizarea informației necesare pentru elaborarea rapoartelor lunare privind contribuțiile de asigurare socială de stat obligatorii (forma IPC 18) și rapoartelor trimestriale privind primele de asigurare

obligatorie de asistență medicală (forma IPC 18); h) Întocmirea, lunară, a declarației persoanei asigurate REV 5 pentru fiecare angajat și transmiterea acestora Casei Teritoriale de Asigurări Sociale, în format electronic prin SIA EREPORTING cu aplicarea semnăturii digitale; i) Asistarea procesului (prin furnizarea informației necesare) pentru completarea periodică (lunară) a raportului și dării de seamă privind venitul achitat și impozitul pe venit reținut din acesta; j) Completarea lunară, trimestrială și anuală a dărilor de seamă cu prezentarea acestora Inspectoratului Fiscal de Stat, precum și perfectarea și eliberarea informației privind veniturile calculate și achitate în folosul persoanei fizice și impozitul pe venit reținut din aceste venituri angajaților; k) Prelucrarea cererilor și a documentelor confirmative privind acordarea scutirilor la impozitul pe venit reținut din salariu, în conformitate cu capitolul 4, titlul II din Codul Fiscal; l) Eliberarea certificatelor de salariu, la cererea angajaților; m) Completarea și stocarea fișelor personale de evidență a veniturilor sub formă de salariu și alte plăți efectuate de către patron în folosul angajatului pe fiecare an, precum și a impozitului pe venit reținut din aceste plăți (Anexa nr. 8 la Ordinul IFPS nr.676 din 14.12.2007); n) Emiterea, transmiterea si primirea documentelor financiar-contabile (facturi, anexe la facturi, documente justificative, acte de prestare servicii); o) Prezentarea documentelor financiare ce conțin date cu caracter personal către acționari/fondatori, comisiei de cenzori, auditului intern sau extern.

În cazul datelor cu caracter personal ale angajaților sau ale altor persoane, primăria orașului Rezina se află în relație juridică, îi va înștiința pe aceștia atunci când datele respective vor fi transmise către terți;

2.5. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate astfel încît să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămîne la păstrare primind statut de document de arhivă.

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

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ CONTABILĂ

3.1. Datele cu caracter personal conținute în sistemul de evidență contabilă în cadrul primăriei orașului Rezina se prelucrează/stochează: pe suport de hîrtie și în format electronic.

3.2 Prelucrarea informațiilor în sistemul de evidență contabilă pe suport de hîrtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri, care sînt amplasate fizic în biroul contabilității primăriei orașului Rezina.

3.3. Mentenanța programului contabil este efectuată de către compania autorizată fiind încheiat contract privind prestarea serviciilor informatice, cu următoarele principalele 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; - Examinarea solicitărilor parvenite din partea primăriei orașului Rezina; - Vizite la fața locului, la solicitarea primăriei.

Examinarea și nedivulgarea informației cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

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 orașului Rezina.

4.2. La expirarea termenilor menționați, datele din sistemul de evidență contabilă sînt păstrate în formă arhivată, pe perioada stabilită, ulterior fiind supuse distrugerii sau ștergerii, în funcție de suportul pe care au fost efectuate.

V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. Primăria orașului Rezina, 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 protecţie a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenţie, de opoziţie asupra datelor cu caracter personal ce-i vizează, precum şi dreptul de a se adresa în justiţie.

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

5.4. Acordarea dreptului de acces a angajaţilor la informaţiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii primăriei oraşului Rezina. Informaţiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum şi perioada concretă pentru care solicită informaţiile.

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 informaţiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţămîntul 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 hîrtie 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 softurile destinate prelucrării acestora sînt 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 ţinînd 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, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspîndirea 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 sînt amplasate în locuri cu acces limitat pentru persoane străine.

6.11. Uşile şi ferestrele sînt 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.

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

6.15. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă contabilă, sînt protejate contra conectărilor nesancţionate sau deteriorărilor.

6.16. 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 sînt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lîngă cerinţele de păstrare a confidenţialităţii parolelor, este interzisă înscrierea acestora pe suport de hîrtie, 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. 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.

7.5. 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 evidenţă contabilă, încetează automat la expirarea perioadei stabilite în timp (pentru iecare tip de cont de acces în parte).

7.6. 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.

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

7.8. Se impun limite în privinţa persoanelor care au dreptul: a) să vizualizeze informaţiile stocate în sistemul de evidenţă contabilă; b) să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

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

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

7.11. Orice încălcare a securităţii în ceea ce priveşte sistemul de evidenţă contabilă este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cît de urgent posibil.

7.12. Înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea sistemului de evidenţă 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 evidenţă 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 informaţiilor din sistemele de evidenţă 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 informaţiilor din sistemul de evidenţă 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, sînt 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 evidenţă 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, preîntîmpinarea, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidenţă contabilă.

10.3. „În cazul producerii incidentelor de securitate persoanele responsabile va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia 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. Totodată, în cadrul controalelor efectuate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar şi să asigure accesul la informaţiile necesare relevante obiectului controlului."

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

XI. DISPOZIŢII FINALE

11.1. Prezentul Regulament este revizuit şi ulterior aprobat de către consiliul orăşenesc periodic, precum şi la necesitate.

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

11.3. Regulamentul este adus la cunoştinţa angajaţilor primăriei şi instituţiilor din subordine contra semnăturii.

Secretara consiliului orăşenesc Rezina Lilia Răileanu