

Republica Moldova  
PRIMARUL  
municipiului Orhei  
MD-3500, mun. Orhei, str. V.Mahu, 160  
tel: +373 235 22767; fax: +373 235 20378  
email: primaria@orhei.md  
www.orhei.md



REGULAMENTUL  
PRIVIND PRELUCRAREA INFORMATIILOR CE CONTIN DATE  
CU CARACTER PERSONAL IN SISTEMUL DE EVIDENȚĂ  
CENTRUL DE INFORMARE ȘI PRESTĂRI SERVICII  
DIN CADRUL PRIMĂRIEI MUNICIPIULUI ORHEI

**DISPOZIȚIE**

27.11.2018

nr. 335

Cu privire la aprobarea și implementarea prevederilor Regulamentului privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei

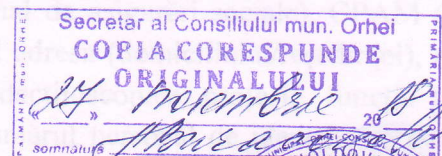
Conform prevederilor Legii nr.133 din 8 iulie 2011 cu privire la protecția datelor cu caracter personal, Hotărârii Guvernului nr.1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, în temeiul art. 29 și art. 32(1) din Legea nr. 436-XVI din 28.12.2006 privind administrația publică locală, Primarul municipiului Orhei DISPUNE:

1. Se aprobă Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei, conform anexei anexei la prezenta dispoziție.
2. Controlul executării prevederilor prezentei dispoziții revine viceprimarilor municipiului Orhei, conform domeniilor de competență.
3. Prezenta dispoziție intră în vigoare la data includerii ei în Registrul de stat al actelor locale.

Primar



Ilan ȘOR



**REGULAMENTUL**  
**PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE**  
**CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ**  
**CENTRUL DE INFORMARE ȘI PRESTĂRI SERVICII**  
**DIN CADRUL PRIMĂRIEI MUNICIPIULUI ORHEI**

**I. DISPOZIȚII GENERALE**

1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei (în continuare Regulament) este elaborat în vederea implimentării în cadrul a prevederilor Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal și a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010.
2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale subiecților de date cu caracter personal în cadrul sistemului de evidență a Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei.

**II. SCOPUL, CATEGORII DE DATE PRELUCRATE**

1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență a Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei constă în asigurarea organizării și coordonării activității Consiliului municipal Orhei, Primăriei municipiului Orhei și Centrului de Informare și Prestări Servicii inclusiv exercitarea după caz, a altor sarcini de bază și/sau delegate de către angajații Primăriei municipiului Orhei conform legislației în vigoare.
2. **În cadrul sistemului de evidență a Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei sînt prelucrate următoarele categorii de date cu caracter personal:** numele, prenumele, patronimicul datele membrilor de familie, sexul porecla/pseudonimul, data și locul nașterii cetățenia, semnătura semnătura digitală, date din actele de stare civilă date din permisul de conducere, date din certificatul de înmatriculare sancțiuni disciplinare, nr. dosarului de pensie CPAS (codul personal de asigurări sociale), CPAM (codul personal de asigurări medicale) telefon/fax, telefon mobil adresa (domiciliului/reședinței), e-mail date genetice, date biometrice sau antropometrice date dactiloscopice, profesie, funcție loc de muncă, formare profesională - diplome- studii IDNP (numărul personal de identificare de stat), situație familială situație militară, situație economică sau financiară date privind bunurile deținute, date bancare obișnuințe/preferințe/comportament, imagine voce, date de geolocalizare/trafic

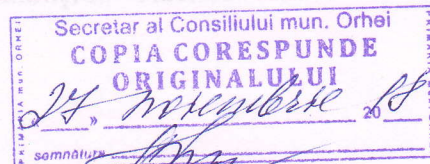
caracteristici fizice, originea rasială originea etnică, convingerile politice convingerile religioase, date privind starea de sănătate date privind viața sexuală, date referitoare la condamnări penale convingerile filosofice, apartenența socială măsurile procesuale de constrângere, sancțiunile contravenționale și, exercitarea după caz, a altor sarcini de bază și/sau delegate de către angajații Primăriei municipiului Orhei.

3. **Prelucrarea datelor cu caracter personal menționate va fi efectuată pentru realizarea următoarelor scopuri:** rapoarte de credit, evidența electorală, evidența populației sau stare civilă, gestiune economico-financiară sau administrativă, protecție sau asistență socială, reclamă, marketing sau publicitate, selecție sau plasare a forței de muncă, servicii de reprezentare în justiție, servicii de telecomunicații electronice, prevenirea, cercetarea, combaterea infracțiunilor, menținerea ordinii publice, securității statului, ținerea de registre de stat, taxe sau impozite, urbanism sau amenajarea teritoriului, evaluarea credibilității, evaluarea altor aspecte ale personalității (nu competență profesională, credibilitate, comportament), analizarea faptelor susceptibile de a atrage răspundere disciplinară, analizarea faptelor susceptibile de a atrage răspundere penală, cadastru sau administrare imobiliară, colectare debite/recuperare creanțe, servicii financiar-bancare, eliberare autorizații / licențe, evidența de fond funciar, monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor, educație sau cultură, resurse umane, servicii hoteliere sau de turism, constatarea sau sancționarea contravențiilor, statistica, tranzacții imobiliare, evaluarea competenței profesionale, evaluarea comportamentului, analizarea solvabilității / situației, economico-financiare, analizarea faptelor susceptibile de a atrage răspundere contravențională și, exercitarea după caz, a altor sarcini de bază și/sau delegate de către angajații Primăriei municipiului Orhei.
4. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență al populației în alte scopuri decât cele menționate mai sus este interzisă.

### III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ CENTRUL DE INFORMARE ȘI PRESTĂRI SERVICII DIN CADRUL PRIMĂRIEI MUNICIPIULUI ORHEI

1. Datele cu caracter personal conținute în sistemul de evidență a Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei se prelucrează/stochează:
  - a) pe suport de hârtie - formulare îndeplinite, chestionare, dări de seamă lunare/trimestriale/semianuale, rapoarte, registre, completate manual, avize ale comisiilor consultative a consiliului municipal Orhei, procese verbale ale consiliului municipal Orhei, ale ședințelor/grupurilor de lucru instituite prin dispoziția autorității executive, citații, hotărâri de aplicare a sancțiunii contravenționale, procese verbale cu privire la contravenții întocmite de către agenții constatatori agenților constatatori desemnați
  - b) în format electronic – în computerul care se află în biroul Centrului de Informare și Prestări Servicii, birourile angajaților din cadrul Primăriei municipiului Orhei.

### IV. PERSOANA RESPONSABILĂ



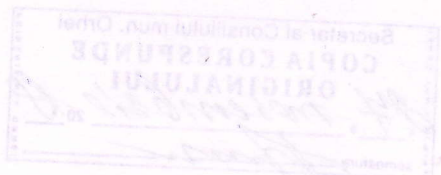
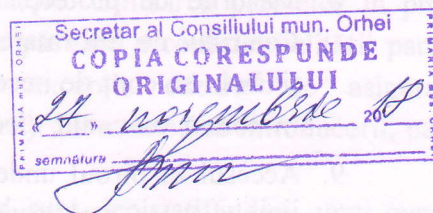
Specialistul din cadrul Primăriei municipiului Orhei este persoana responsabilă de prelucrarea datelor cu caracter personal numită prin dispoziția primarului/viceprimarului municipiului Orhei.

## V. DURATA DE STOCARE

Prelucrarea datelor cu caracter personal în sistemul de evidență se efectuează în cadrul Primăriei și se păstrează potrivit nomenclatorului dosarelor primăriei mun. Orhei coordonat cu Serviciul Raional de Arhivă Orhei.

## VI. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

1. În calitate de operator de date cu caracter personal Primăria municipiului Orhei, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.
2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.
3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență vor respecta procedura de acces la datele cu caracter personal.
4. Acordarea dreptului de acces a angajaților la informațiile ce vizează populația municipiului Orhei se efectuează prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii. Informațiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.
5. Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu, dacă în informațiile solicitate apar și alte persoane și nu există posibilitatea de a obține consimțământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

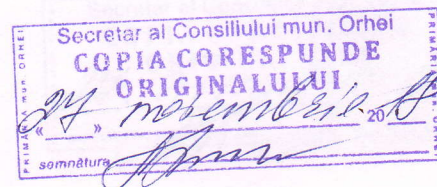


**VII. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL  
PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ  
CENTRUL DE INFORMARE ȘI PRESTĂRI SERVICII  
DIN CADRUL PRIMĂRIEI MUNICIPIULUI ORHEI**

1. Cerințe speciale față de marcare: toate informațiile ieșite din sistemul de evidență a Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

*Model Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr. 000000X-00X, înregistrat în Registrul de evidență al operatorilor de date cu caracter personal [www.registru.datepersonale.md](http://www.registru.datepersonale.md). Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.*

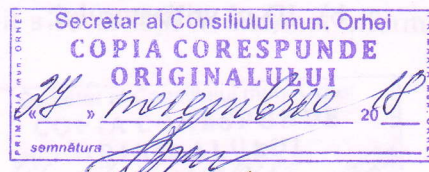
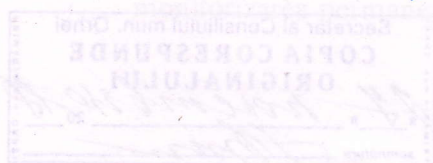
2. În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronic, care conțin date cu caracter personal, aceștia se păstrează în safeuri /dulapuri cu acces restricționat.
3. La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.
4. Utilizatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.
5. Accesul fizic la informațiile prelucrate în cadrul Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei este blocat împotriva vizualizării de către persoane neautorizate - Regula mesei curate.
6. Mijloacele de prelucrare a informațiilor personalizate prelucrate sau softurile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
7. Scoaterea și introducerea mijloacelor de prelucrare a informațiilor /în perimetrul de securitate se înregistrează în registru.
8. Măsurile de protecție a datelor cu caracter personal, prelucrate în cadrul prelucrate în cadrul Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei, se înfăptuiesc ținându-se cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție : în formă manuală, electronică și externă.
9. Accesul în biroul unde sunt amplasate datele cu caracter personal, utilizate în cadrul activității specialiștilor, este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program. Accesul în birouri este posibil doar cu autorizarea de acces și cheia de la lacătul mecanic.
10. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se va încuia.
11. Registrele de monitorizare a accesului la informațiile personalizate (eliberarea actelor și sau informațiilor ce conțin date cu caracter personal) se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă.



12. Perimetrul de securitate se consideră perimetrul biroului în care sunt amplasate datele cu caracter personal din cadrul sistemului de evidență al populației, fiind integru din punct de vedere fizic.
13. Zilnic, paznicii inspectează perimetrul de securitate al clădirii și al biroului, unde sunt amplasate datele cu caracter personal, din punct de vedere fizic.
14. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine. Ușile și ferestrele sunt încuiate în cazul în care în încăperea nu sunt angajații, utilizatorii.
15. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței unei permisiuni speciale a conducerii deținătorului de date cu caracter personal.
16. Amplasarea datelor cu caracter personal din cadrul sistemului de evidență - Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
17. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență al populației, sunt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaționale.

#### **VIII. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENȚĂ CENTRUL DE INFORMARE ȘI PRESTĂRI SERVICII DIN CADRUL PRIMĂRIEI MUNICIPIULUI ORHEI**

1. Este efectuată identificarea și autentificarea utilizatorilor informațiilor prelucrate în cadrul Centrului de Informare și Prestări Servicii din cadrul Primăriei municipiului Orhei și a proceselor executate în numele acestor utilizatori.
2. Toți utilizatorii (inclusiv personalul care asigură mentenanța tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmamentele nivelului de accesibilitate al utilizatorului.
3. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepția cazului de asigurare a securității păstrării acestora (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.
4. Se efectuează modificarea parolelor de fiecare dată când sunt depistați indicii unei eventuale compromiteri a sistemului sau parolei.
5. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sunt folosiți identificatori și parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora. După cinci tentative greșite de autentificare, accesul este blocat, în mod automat.



6. Se asigură, pentru o perioadă de 1 (unu) an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor și prevenirea folosirii repetate a acestora.
7. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate și, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum și în caz de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizații de acces primite în scopul comiterii unei fapte prejudiciabile, absență a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare și autentificare se revocă sau se suspendă.
8. În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuiesc cu regularitate, maximum la fiecare șase luni și după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor.
9. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autorizează de persoanele responsabile.
10. Toți angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor cu caracter personal.
11. Orice încălcare a securității în ceea ce privește protejării datelor cu caracter personal este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât mai urgent posibil.
12. Înainte de acordarea accesului la datele cu caracter personal ale populației, utilizatorii sunt informați despre faptul că sistemul informațional al datelor cu caracter personal este controlat și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

#### **IX. AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ CENTRUL DE INFORMARE ȘI PRESTĂRI SERVICII DIN CADRUL PRIMĂRIEI MUNICIPIULUI ORHEI**

1. Primaria municipiului Orhei organizează generarea înregistrărilor de audit a securității în sistemul informațional de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.
2. Înregistrările de audit a securității registrelor ținute manual în care sînt prelucrate date cu caracter personal, trebuie să conțină:
  - a) numele și prenumele utilizatorului;
  - b) numele fișei accesate (pagina și inscripția din registru);
  - c) numărul înregistrărilor efectuate;
  - d) tipul de acces;
  - e) data accesului (an, lună, zi);
  - f) timpul (ora, minuta) și durata accesului
3. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
  - a) data și timpul tentativei intrării/ieșirii;
  - b) ID-ul utilizatorului;

- c) rezultatul tentativei de intrare/ieșire – pozitivă sau negativă.
4. Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:
- a) data și timpul tentativei de pornire;
  - b) denumirea/identificatorul programului aplicativ sau al procesului;
  - c) ID-ul utilizatorului;
  - d) rezultatul tentativei de pornire – pozitivă sau negativă.
5. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
- a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
  - b) denumirea (identificatorul) aplicației sau a procesului;
  - c) ID-ul utilizatorului;
  - d) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
  - e) tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
  - f) rezultatul tentativei de obținere a accesului (executare a operațiunii) – pozitivă sau negativă.
6. Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
- a) data și timpul modificării competențelor;
  - b) ID-ul administratorului care a efectuat modificările;
  - c) ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
7. 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:
- a) data și timpul eliberării;
  - b) denumirea informației și căile de acces la aceasta;
  - c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
  - d) ID-ul utilizatorului care a solicitat informația;
  - e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.
8. În caz de deranjament al auditului securității în sistemul informațional de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal și sunt întreprinse măsuri în vederea restabilirii capacității de lucru a sistemului de audit. Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemul informațional



de date cu caracter personal, în scopul depistării activităților neobișnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul, și întreprinderea acțiunilor prestabilite în politica de securitate pentru astfel de cazuri.

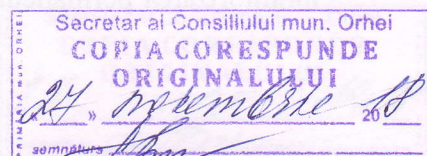
9. Rezultatele auditului securității în sistemul informațional de date cu caracter personal, care reprezintă operațiuni de prelucrare a datelor cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității și integrității acestora. Durata stocării rezultatelor auditului securității în sistemul informațional de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar, în orice caz, acest termen nu este mai mic de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigațiile sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

#### **X. ASIGURAREA INTEGRITĂȚII INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ CENTRUL DE INFORMARE ȘI PRESTĂRI SERVICII DIN CADRUL PRIMĂRIEI MUNICIPIULUI ORHEI**

1. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestor soft-uri, protecția contra infiltrării programelor dăunătoare în soft-uri, măsură care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.
2. Se utilizează tehnologii și mijloace de constatare a intrărilor ilegale, care permit monitorizarea evenimentelor și constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemului informațional de date cu caracter personal.
3. Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemului informațional de date cu caracter personal (automat - la pornirea sistemului și lunar - la solicitarea utilizatorului autorizat în acest scop).

#### **XI. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE DE EVIDENȚĂ CENTRUL DE INFORMARE ȘI PRESTĂRI SERVICII DIN CADRUL PRIMĂRIEI MUNICIPIULUI ORHEI**

1. Personalul care asigură exploatarea sistemului informațional de date cu caracter personal trece minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.
2. Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Incidentele de securitate a sistemului informațional de date cu caracter personal se urmăresc și se documentează în regim permanent.



3. Anual, către 31 ianuarie, Primaria municipiului Orhei prezintă Centrului național pentru protecția datelor cu caracter personal raportul generalizat despre incidentele de securitate a sistemului informațional de date cu caracter personal din instituție. În baza acestui raport Centrul întreprinde măsurile ce se impun de Legea cu privire la protecția datelor cu caracter personal.
4. Persoanele împuternicite de către operator și alte persoane vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția datelor personale ale salariaților din instituție poartă răspundere disciplinară, materială, contravențională și penală în modul prevăzut de legislația în vigoare.

## XII. DISPOZIȚII FINALE

1. Prezentul Regulament este revizuit și ulterior aprobat de către primar/viceprimar al municipiului Orhei, periodic, însă cel puțin o dată în an, precum și la necesitate.
2. Prezentul Regulament se completează cu prevederile legislației în vigoare.
3. Regulamentul este adus la cunoștința angajaților contra semnăturii.
4. Modificarea și completarea prezentului Regulament se va efectua în modul stabilit pentru aprobarea lui.

Secretar al Consiliului mun. Orhei  
COPIA CORESPUNDE  
ORIGINALULUI  
24 noiembrie 2015  
semnătura

