PROIECT

DECIZIA

nr. 20 din _____ 2018

Cu privire la aprobarea politicii de securitate privind protecția datelor cu caracter peresonal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Primăria oraşului Sîngerei.

În scopul protecției datelor cu caracter personal, în conformitate prevederile Legii nr. 133 din 18.07.2011 cu privire la protecția datelor cu caracter personal, conform art. 14 alin. 2 lit. z^1 din Legea nr. 436-XVI din 28.12.2006 „privind administrația publică locală", Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010, Regulamentul Registrului de evidență al operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr. 296 din 15 mai 2012, Consiliul orăşenesc Sîngerei **DECIDE:**

1. Se aprobă Regulamentul politicii de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Primăria oraşului Sîngerei, conform *anexei nr.1.*
2. Controlul executării prezentei decizii se pune în sarcina comisiei consultative pentru domeniile sociale (dna. L.Hajevschi).

Autorul proiectului Lucia Baciu

Coordonat:

Primarul or.Sîngerei Gheorghe Braşovschi

Jurist Galina Afanasiev

Notă: În conformitate cu Legea privind APL nr.436-XVI din 28.12.2006, art.19 (3,4) proiectul în cauză se adoptă cu votul majorității consilierilor aleşi (12).

Anexa nr.1 la Decizia consiliului

nr._____ din _____2018

POLITICA DE SECURITATE
PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR INFORMAȚIONALE GESTIONATE DE PRIMĂRIA ORAȘULUI SÎNGEREI

I. Preambul

La prelucrarea datelor cu caracter personal în cadrul Primăriei orașului Sîngere sînt aplicate principiile prevăzute de 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 Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010, Regulamentului Registrului de evidență al operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr. 296 din 15 mai 2012, și alte acte legislative/normative de profil.

II. Introducere

Prezenta Politică de Securitate este aprobată de către Consiliul orășenesc Sîngerei, care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru protecția datelor, ținîndu-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sînt expuse acestea.

III. NOȚIUNI GENERALE

În prezenta Politică de Securitate, 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 şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor primite de la operator;

autentificare - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

control de securitate - acţiuni întreprinse de către APL în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute;

fişiere temporare - ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat pînă la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare - atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

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

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

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

politica de securitate a datelor cu caracter personal - document, 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– orice manifestare de voinţă liberă, expresă şi necondiţionată, în formă scrisă sau electronică, conform cerinţelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;
depersonalizarea datelor – modificarea datelor cu caracter personal astfel 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.

IV.Obiectivile Politicii de Securitate

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de APL, atît în cadrul prelucrării manuale, cît şi sistemelor şi proceselor de tehnologie informaţională.

V.Responsabilitatea persoanei responsabile de Politica de securitate

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

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

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

VI.Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:

1.Preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele,

2.excluderea accesului neautorizat la datele cu caracter personal prelucrate;

3.preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program,

4.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.

VII.Măsurile generale de administrare a securităţii informaţionale:

1.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.

2.Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.

3. 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.

VIII.Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal

1.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

2.Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc membrii.

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

4.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.

5.Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul desecuritate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii.

IX.Utilizarea parolelor în procesul asigurării securităţii informaţionale

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

- păstrarea confidenţialităţii parolelor,
- interzicerea înscrierii parolelor pe suport de 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.

X.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.

XI.Controlul instalării şi scoaterii componentelor T.I.

Informaţiile, care conţin date cu caracter personal , se distrug fizic sau se transcriu şi se nimicesc prin metode sigure.

XII.Dezvăluirea datelor cu caracter personal

1 Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale sînt interzise.

2. Acces la sistemele informaționale gestionate în cadrul Primăriei orașului Sîngerei, din partea Procuraturii , Inspectoratului de Poliție, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212 Cod de procedură penală.

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

1. Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă.

2. 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.

XIV.Auditul sistemelor informaționale gestionate

Responsabilul de administrarea sistemului este obligat să efectuieze următoarele procedeie de audit :

a) Să efectuieze înregistrarea tentativelor de întrare/ieșire în sistem, conform următorilor parametri:

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

b) Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal,conform următorilor parametri:
- data și timpul tentativei de obținere a accesului (executate a operațiunii),
- denumirea (identificatorul) aplicației sau procesului, o ID-ul utilizatorului,
- specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.),
- tipul operațiunii solicitate (citire, înregistrare, ștergere etc.),
- rezultatul tentativei de obținere a accesului (executare a operațiunii) — pozitivă sau negativă.

c) Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
- data și timpul modificării competențelor,
- ID-ul administratorului care a efectuat modificările,

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

d) Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

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

XV.Asigurarea protecţiei contra programelor dăunătoare (viruşilor)

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

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

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

XVII.Gestionarea incidentelor de securitate

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

2.Pînă la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrul Național pentru Protecția Datelor cu Caracter Personal despre incidentele de securitate constatate.