APROBAT

Prin dispoziția primarului nr. 46 din 08.08.2024

OLEG COCIERU

POLITICA PRIVIND RESURSELE INFORMATICE ÎN CADRUL PRIMĂRIEI SATULUI LUNGA

1. DEFINIȚII

„date cu caracter personal" - orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

„prelucrare" - înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

„operator" - reprezintă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin actele normative, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în actele normative;

„persoană împuternicită de operator" - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

„destinatar" - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

„parte terță" - înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

„consimțământ" - al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

„încălcarea securității datelor cu caracter personal" - înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate
într-un alt mod, sau la accesul neautorizat la acestea;

2. CADRUL GENERAL

Scop. Prezenta politică are ca scop asigurarea securității resurselor informaționale ale **PRIMĂRIEI SATULUI LUNGA .**

(în continuare **"Operator"** sau **"entitatea")**. Se va urmări protecția resurselor informaționale împotriva modificărilor neautorizate sau accidentale, asigurând acuratețea și completitudinea acestora, precum și protecția resurselor informaționale împotriva divulgării neautorizate.

3. DOMENIUL DE APLICARE

Prezenta politică se aplică tuturor structurilor organizatorice/departamentelor Operatorului de date **PRIMĂRIA SATULUI LUNGA .**
Prezenta politică va fi considerată ca având caracter general și se va aplica tuturor prelucrărilor efectuate de Operator. În cazul în care se constată existența anumitor aspecte legate de gestionare datelor cu caracter general pentru care prezenta politică nu oferă directive corespunzătoare, angajații trebuie să solicite imediat consiliere din partea Responsabilului pentru Protecția Datelor (DPO), dacă a fost numit, sau reprezentantului legal al Operatorului.

4. PREVEDERI GENERALE

4.1. Principii. Toți angajații și prestatorii de servicii care utilizează resursele informaționale ale Operatorului de date **PRIMĂRIA SATULUI LUNGA** au responsabilitatea de a proteja activele informaționale ale Operatorului, folosind prezenta politică drept un instrument principal și aderând la standardele, procedurile și îndrumările incluse în acesta.

Rețelele, aplicațiile și sistemele informatice ale Operatorului sunt disponibile în momentul în care este nevoie de ele. Acestea nu pot fi accesate decât de către utilizatorii autorizați și conțin informații corecte și complete.

Prin implementarea unor măsuri atât tehnice, cât și operaționale, Operatorul va proteja toate programele, echipamentele și activele informaționale aflate în patrimoniul ei.

4.2. Informarea utilizatorilor. Fiecare angajat/prestator de servicii care utilizează resursele informaționale ale Operatorului de date **PRIMĂRIA SATULUI LUNGA,** va participa în momentul angajării și ulterior, anual, la cursuri de securitate a informațiilor organizate de conducerea Operatorului. De asemenea, fiecărui angajat/prestator de servicii îi vor fi puse la dispoziție, în momentul angajării/semnării contractului de colaborare, copii ale prezentei politici, precum și ale tuturor normelor și procedurilor operaționale IT, pe care va trebui să le respecte. Aceștia își vor exprima acordul cu privire la respectarea acestor norme prin semnarea formulatorului din **Anexa 1** a acestui document.

De asemenea, prezenta politică precum şi celelalte norme şi proceduri operaţionale IT vor fi postate pe Intranetul Operatorului într-o locaţie disponibilă tuturor angajaţilor. Angajaţii vor fi informaţi cu privire la această locaţie. Prezenta politică precum şi celelalte procedurii operaţionale se adresează deopotrivă şi prestatorilor de servicii ai Operatorului, care vor folosi sau vor avea acces la resursele fizice şi informaţionale ale Operatorului. Pentru a dovedi luarea la cunoştinţă a prevederilor incluse în aceste norme, colaboratorii vor semna formularul din **Anexa 1.**

4.3. Evaluarea riscurilor. Operatorul realizează în mod continuu evaluarea riscurilor pentru toate sistemele informatice, aplicaţiile şi reţele care sunt utilizate în cadrul tuturor proceselor Operatorului. Totodată, se vor identifica măsurile necesare pentru protecţia împotriva breşelor de confidenţialitate, integritate şi disponibilitate.

4.4. Utilizarea informaţiilor. Fiecare angajator/ prestator de servicii care utilizează resursele informaţionale ale Operatorului de date **PRIMĂRIA SATULUI LUNGA** trebuie să aibă acces doar la informaţia necesară pentru a-şi îndeplini sarcinile. Informaţiile sensibile trebuie accesate doar de către angajaţii / prestatorilor de servicii cărora proprietarul aplicaţiei respective le-a acordat drept de acces.

Informaţiile Operatorului nu trebuie folosite în alte scopuri decât cele de afaceri aprobate în mod oficial de către Conducere. Folosirea neaprobată a informaţiilor Operatorului este interzisă.

Utilizatorilor nu le este permis să efectueze nicio activitate în sistemele informatice ale Operatorului ce ar putea conduce la deteriorarea imaginii Operatorului.

Folosirea în scop personal a informaţiilor Operatorului, cum ar fi listele de distribuţie a e-mail-urilor, este interzisă.

Nu este permisă utilizarea de programe licenţiate de către Operator pe calculatoare personale, cu excepţia cazului în care sistemul a fost desemnat să proceseze informaţii ale Operatorului.

Toate activităţile utilizatorilor sunt înregistrate şi analizate ulterior. O conduită nepotrivită poate duce la acţiuni disciplinare inclusiv revocarea drepturilor de acces. Operatorul permite utilizarea ocazională a sistemelor informatice în scop personal, inclusiv a telefonului, atât timp cât nu implică costuri semnificative, nu interferează cu performanţa la locul de muncă, şi nu limitează accesul altor utilizatori la resursele sistemului.

4.5. Politica pentru parole

Accesul la sistemul informatic al Operatorului trebuie să fie restricţionat pe bază de nume de utilizator şi parolă.

Parolele asociate conturilor de utilizatori nu trebuie folosite pentru autentificarea în sisteme externe (de ex. Conturi personale de e-mail, conturi pe site-uri comerciale etc.). Parolele trebuie să difere de la o aplicaţie accesată la alta. Alegeţi parole diferite pentru aplicaţii faţă de cele pentru accesul în reţea.

Utilizatorii nu trebuie să dezvăluie nimănui parolele utilizate în cadrul sistemelor informatice ale Operatorului, nici măcar celorlalţi angajaţi. Toate parolele sunt calificate ca informaţii confidenţiale.

Nu este permisă stocarea parolelor în sistemele informatice. Nu este permisă scrierea parolelor în clar pe hârtie sau pe un alt suport.

Pentru protejarea parolelor, utilizatorii trebuie să:

- NU destăinuie sub nicio circumstanță nicio parolă NIMĂNUI;
- NU împărtășească parolele cu membrii familiei;
- NU dezvăluie parola colegilor de serviciu pe perioada concediului;
- NU ofere NIMĂNUI detalii cu privire la parolă („numărul meu de la mașină");
- NU scrie în clar parola pe hârtie sau în mesaje electronice;
- NU păstreze parolele scrise;
- NU stocheze parolele sub formă de fișiere pe NICIUN sistem de calcul (nici pe echipamentele mobile) fără ca acele fișiere să fie criptate;

Este necesar ca utilizatorii să schimbe parola cel puțin o dată la 90 de zile. Dacă un utilizator suspectează că o persoană a aflat un cont de utilizator sau o parolă ce nu ii este atribuită, trebuie să raporteze departamentului IT și să-și schimbe imediat parola în cazul în care aceasta este la cauză.

Parolele adecvate au următoarele caracteristici:

- conțin atât majuscule, cât și litere mici (A-Z, a-z);
- conțin cifre și cel puțin un caracter alfanumeric (0-9,!@#$%^&*()_+:?;.);
- nu se bazează pe informații personale precum nume, numere de telefon etc.;
- nu coincid și nu conțin numele de utilizator;
- au lungimea minimă de opt caractere.

Parolele neadecvate reprezintă parole cu grad scăzut de complexitate ce sunt deseori caracterizate de una dintre următoarele specificații:

- reprezintă un cuvânt folosit în mod uzual, cum ar fi:
  - numele de familie al utilizatorului, numele copiilor, colegilor de serviciu, animalelor de Operator etc.;
  - zilele de naștere, adrese, numere de telefon, numărul de la mașină sau alte informații personale;
  - cuvinte sau succesiuni de litere sau cifre de genul: abcdef,123456,zyxwvuts, 123321 etc.;
  - oricare dintre cuvintele de mai sus scrise în ordinul invers;
- coincid sau conțin numele de utilizator;
- au lungimea mai mică de opt caractere.

4.6. Accesul la distanță

Accesul la distanță se va face folosind un mecanism de autentificare cu parolă valabilă o singură dată sau prin chei publice/private protejate cu parole corespunzătoare. Accesul la distanță se acordă după aprobarea Departamentului IT și conducătorului Operatorului.

Accesul de la distanță în sistemele Operatorului impune respectarea următoarelor reguli:

- Remote control – descriere proces de acces sistem (se identifică partea care încearcă să acceseze, se comunică parola de acces prin telefon, nu e-mail: parola de acces este regenerată la fiecare logare).
- Înainte de a iniția conexiunea la rețeaua Operatorului, angajații trebuie să se asigure că echipamentul de calcul pe care îl folosesc nu este conectat în același timp la o altă rețea.

- Orice altă configurație hardware sau sotfware de acces de la distanță în afara celor agreate de Operator trebuie aprobată de Departamentul IT.
- Conectarea de la distanță la rețeaua Operatorului implică folosirea unui software antivirus agreat și actualizat zilnic la ultimele semnături de virusuri.
- Angajații vor accesa sistemele Operatorului de la distanța numai folosind echipamentele Operatorului, configurate și protejate corespunzător (PC-uri, Laptopuri, PDA-uri, tablete etc.), sau după caz, în cazuri excepționale folosind echipamentele personale, doar cu autorizarea conducătorului.

4.7. Raportarea incidentelor

Angajații trebuie să raporteze toate incidentele cu privire la sistemele informatice ale Operatorului, iar cele referitoare la securitatea informației trebuie să fie raportate Departamentului IT.

Angajații vor raporta incidentele întâlnite către responsabilii din cadrul Operatorului prin trimiterea unui mesaj electronice în care vor specifica condițiile de apariție ale incidentului, alături de toate detaliile observate la momentul procedurii.

Procesul de raportare a incidentelor de securitate a informației folosește aceleași căi de raportare ca și în cazul incidentelor obișnuite.

5. ROLURI ȘI RESPONSABILITĂȚI

5.1. Angajații

Toți angajații care activează în cadrul Operatorului au următoarele responsabilități:

- să respecte Politica privind resursele informatice;
- să asiste în sesiuni de informare și la cursuri de securitatea informației;
- să se familiarizeze și să acționeze în concordanță cu toate cerințele Operatorului referitoare la securitatea informației;
- să solicite șefului lor direct acces la resursele informaționale care le sunt necesare;
- să raporteze toate activitățile suspecte și problemele de securitate;
- să raporteze orice suspiciune de breșă de securitate sau breșă de securitate ca atare;
- să prevină introducerea în sistemele informaționale din cadrul Operatorului de produse software cu potențial distructiv;
- să păstreze în bună stare resursele informaționale, produsele software și echipamentele hardware ale Operatorului.

5.2. Conducerea Operatorului

Are următoarele responsabilități:

- să asigure securitatea bunurilor organizației (informație, echipamente hardware, produse software folosite de către angajați și de către terțe părți);
- să asigure aplicarea politicii de securitate a Informației;
- să se asigure că toți angajații sunt conștienți de responsabilitățile de securitate pe care le au;
- să se asigure raportarea și înregistrarea tuturor incidentelor de securitate;

- să asigure că orice încălcare a securității informației de către angajați este investigată în mod corespunzător;
- să asigure faptul că angajații au fost instruiți corespunzător cu privire la securitatea informației;
- să emită decizii prin care este dispusă cercetarea faptelor angajaților care au încălcat prevederile prezentei proceduri.

6. Dispoziții finale

Răspunderea în cazul încălcării procedurii

Încălcarea prevederilor acestei proceduri poate determina aplicarea unor măsuri disciplinare, inclusiv desfacerea contractului de muncă din motive care țin de persoana angajatului sau chiar răspunderea penală a persoanei care se face vinovată de încălcarea prevederilor prezentei Proceduri, atunci când legile în vigoare o impun.

Prestatorii de servicii care utilizează resursele informaționale ale Operatorului de date **PRIMĂRIA SATULUI LUNGA**, de asemenea poartă răspundere deplină în conformitate cu legislația în vigoare, în cazul în care se face vinovată de încălcarea prevederilor prezentei Proceduri.

În condițiile menționate, lipsa de înțelegere în cazul în care procedura va fi încălcată nu va putea fi invocată de către utilizatorii cărora le este adresată această procedură.

LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE POLITICII PRIVIND RESURSELE INFORMATICE ÎN CADRUL PRIMĂRIEI SATULUI LUNGA

Nr.	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Anexa 1 – Acord de respectare a Politicii de Securitate a Informațiilor în cadrul PRIMĂRIEI SATULUI LUNGA

Numele complet al utilizatorului: _____
Datele de contact: _____

Subsemnatul identificat mai sus, am luat la cunoștință prevederile Procedurii privind resursele informatice și îmi exprim prin semnarea prezentului formular acordul cu privire la următoarele:

- Să respect toate prevederile politicilor și procedurilor existente în cadrul Operatorului, precum și în Politica privind resursele informatice. În acest sens, am luat la cunoștință conținutul tuturor acestor documente.
- Să adopt toate măsurile de precauție necesare în vederea eliminării riscurilor de dezvăluire către persoane neautorizate a informațiilor interne ale Operatorului sau a informațiilor care mi-au fost încredințate de către Operator.
- Să returnez odată cu finalizarea activității mele pentru Operator, toate materialele la care am primit acces ca rezultat al activității mele în cadrul acesteia. Înțeleg faptul că îmi este interzisă folosirea acestor informații în scopuri personale și nici nu am autorizarea de a dezvălui aceste materiale terților fără aprobarea explicită în scris a managerului desemnat pentru relația cu angajatorul meu din interiorul Operatorului.
- Să informez prompt șeful direct despre orice situație de încălcare sau posibilă încălcare a Politicilor din cadrul Operatorului.
- Sunt de acord cu faptul că încălcarea Politicii privind resursele informatice poate duce la aplicarea de măsuri disciplinare, la revocarea drepturilor, la desfacerea contractului de muncă și eventual la răspunderea legală pe cale civilă sau penală.

Data

Semnătura