APROBAT

Prin dispoziția primarului nr. 46 din 08.08.2024

OLEG COCIERU

Semnătura și Stampila

POLITICA ANTI-SPAM 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 unui nivel adecvat de securitate a sistemelor informaționale ale **PRIMĂRIEI SATULUI LUNGA** (în continuare **"Operator"** sau **"entitatea"**) împotriva SPAM-ului, în principal cu privire la mesajele publicitare nesolicitate și/sau la mesajele ce urmăresc realizarea unei fraude prin obținerea de date confidențiale.

3. DOMENIUL DE APLICARE

Prezenta politică se aplică tuturor structurilor organizatorice/departamentelor ale Operatorului **PRIMĂRIA SATULUI LUNGA** .

4. PREVEDERI GENERALE

4.1. Utilizarea Internetului

Accesul utilizatorilor la Internet este permis pentru îndeplinirea sarcinilor de serviciu.

Utilizatorii nu trebuie să își instaleze niciun produs software pe stațiile de lucru ale Operatorului indiferent de sursa de proveniență a respectivului produs software (Internet sau altă sursă).

Documentele atașate mesajelor e-mail vor putea fi deschise doar dacă acestea sunt primite dintr-o sursă sigură. Înainte de a fi deschise, documentele atașate trebuie scanate cu un program antivirus.

Este interzisă folosirea calculatoarelor Operatorului pentru distribuirea e-mail-urilor nesolicitate ori susținerea oricărui tip de campanie publicitară care ar putea avea ca efect exprimarea unor plângeri din partea destinatarilor.

Mesajele de tip „**SPAM**" includ o varietate de promoții și solicitări precum cele de tipul mesajelor trimise în masă, sistemele piramidale și promovarea directă de produse. Atunci când angajații Operatorului primesc astfel de mesaje vor trebui să le trimită Responsabilului IT fără a le deschide sau a le răspunde. Departamentul IT va adopta măsuri corespunzătoare pentru stoparea primirii acestor mesaje.

În cadrul comunicației electronice se interzice înlocuirea, înlăturarea sau denaturarea identității unui utilizator.

În formularea mesajelor electronice, utilizatorul este obligat să-și precizeze datele de identificare, care trebuie să conțină:

- numele acestuia;
- numărul de telefon;
- adresa de e-mail sau apartenența la o anumită organizație/entitate.

De asemenea, se recomandă atașarea unei semnături electronice în cadrul mesajelor care să conțină informații despre expeditor precum poziția ocupată în cadrul Operatorului, apartenența la aceasta, adresa etc.

Se recomandă confirmarea identității terțelor părți înainte ca angajații Operatorului să poată trimite orice informație de uz intern să încheie orice fel de contract sau să comande produse prin intermediul rețelelor publice. Atunci când este posibil, confirmarea identității trebuie făcută prin intermediul semnăturilor digitale, altfel pot fi utilizate mijloace de identificare complementare: discuții telefonice, scrisoare de împuternicire sau referințe din partea terților.

Nu se permite accesul angajaților în modulul de administrare al site-ului web al Operatorului decât dacă au aprobarea Conducerii de a efectua modificări în conținutul de informații. Adăugarea de legături către alte resurse, actualizarea informațiilor sau schimbarea design-ului intră, de asemenea, sub incidența acestor aprobări.

Acordarea drepturilor de acces din Internet la rețeaua internă a Operatorului se va aproba colaboratorilor numai pe baza unei solicitări exprimate de către managerul de sistem. Din rândul prestatorilor de servicii fac parte: producătorii de software, contractorii, consultații, personalul temporar, personalul companiilor prestatoare de servicii, etc. Accesul va fi acordat în mod individual și doar pentru perioada desfășurării sarcinilor aprobate.

Angajații pot folosi alte surse de furnizare a conexiunii la Internet utilizând calculatoarele Operatorului, doar cu acordul Conducerii, întrucât controalele de acces și metodele de asigurare a securității datelor nu pot fi aplicate corespunzător decât dacă întregul flux de activități referitoare la Internet trece prin echipamentele de tip firewall ale Operatorului. În aceeași manieră, angajații sunt obligați să utilizeze numai căsuța de e-mail oferită de către Operator. În acest context, folosirea adresei de e-mail personale nu este permisă.

Este interzisă folosirea în scopul afacerilor personale sau încredințarea către alte persoane a resurselor informatice ale Operatorului.

Operatorul nu se declară răspunzător pentru conținutul paginilor de Internet accesate de angajați. În cazul accesării întâmplătoare a unui site cu conținut informațional imoral (caracter sexual explicit, rasist, misogin, violent sau de natură ofensatoare), angajații în cauză sunt obligați să aleagă o altă pagină sau să încheie procesul curent.

Operatorul poate înregistra paginile accesate, fișierele desemnate, timpul petrecut pe o pagină anume și alte informații conexe.

Conducerea Operatorului poate primi rapoarte ce conțin astfel de informații și pe baza lor să decidă tipul accesului la Internet în cadrul fiecărui departament al Operatorului.

Conducerea Operatorului are dreptul de a revizui e-mail-urile, fișierele aflate pe stațiile de lucru, fișierele temporare ale browser-elor de Internet (Internet Explorer, Mozilla Firefoc, Google Chrome etc.), paginile marcate, istoricul site-urilor web necesare și alte informații stocate sau care tranzitează stațiile de lucru ale Operatorului în orice moment și fără necesitatea unui anumit prealabil.

Se interzice angajaților stabilirea unor legături la Internet sau la alte rețele externe care ar putea favoriza terțe părți să pătrundă în rețeaua Operatorului și să aibă acces la sistemele și informațiile acesteia, decât dacă acest lucru este aprobat de către Conducere. Aceste conexiuni presupun legături de tip file-sharing (partajare de fișiere), sisteme de comerț prin intermediul Internetului sau servere FTP.

4.2. Utilizarea e-mail-ului

Operatorul pune la dispoziția angajaților săi sau, după caz, prestatorilor de servicii atunci când aceștia utilizează sistemele IT ale Operatorului, căsuțe de poștă electronică. Conturile de poștă electronică individuale nu trebuie utilizate în comun.

Utilizarea sistemului de mesagerie electronică al Operatorului trebuie realizată ca parte a activității profesionale, ce are ca scop îmbunătățirea activităților de zi cu zi prin înlesnirea comunicării interne în cadrul Operatorului, respectiv în exterior prin menținerea legăturilor cu clienții, partenerii de afaceri ai Operatorului sau cu autoritățile locale.

Comunicarea electronică se va limita la materialele care au legătură cu activitățile profesionale și sarcinile de serviciu ale angajaților și nu va fi folosită ca suport pentru campanii caritabile de strângere de fonduri, campanii de susținere politică/religioasă sau pentru activități ce țin de afaceri personale, amuzament sau distracție.

Se interzice folosirea de către un utilizator a unei adrese de e-mail ce aparține altei persoane. Periodic, angajații vor fi informați și instruiți să folosească în mod adecvat resursele sistemului informatic al Operatorului.

În cadrul comunicației electronice se interzice înlocuirea, înlăturarea sau denaturarea identității unui utilizator.

Fiecare utilizator al sistemului de e-mail al Operatorului (administrator sau utilizator final) trebuie să se preocupe de luarea tuturor măsurilor necesare în vederea asigurării protecției împotriva e-mail-urilor nesolicitate (mesaje de tip „hoax", mesaje înlănțuite chain letter, spam etc.) și scheme de mesaje electonice cu caracter fraudulos (phishing și alte tipuri de mesaje de tip fraudulos).

Fiecare utilizator al sistemului de e-mail al Operatorului (administrator sau utilizator final) trebuie să se preocupe de luarea tuturor măsurilor necesare în vederea asigurării protecției împotriva infectării cu produse software cu potențial distructiv (viruși, troieni, worm etc.)

În cazul în care primesc sau detectează orice e-mail suspicios, angajații sunt obligați să informeze Departamentul IT.

4.3. Utilizarea echipamentelor mobile

Toate echipamentele mobile care au fost achiziționate în numele Operatorului sunt considerate a fi proprietatea Operatorului și vor fi utilizate ca atare.

Atribuirea unui dispozitiv mobil către un angajat implică responsabilitatea acestuia de a asigura securitatea dispozitivului atât în sediul Operatorului, cât și în locuința personală sau oricare altă locație.

Accesul la dispozitivele de tip mobile computing trebuie să fie securizat prin sistem de autentificare cu parolă sau cod PIN. Pentru o eficiență sporită nu vor fi folosite parole și coduri PIN ușor de identificat.

Accesul la rețeaua Operatorului din exterior nu este permisă decât printr-o conexiune securizată de tip VPN.

Utilizarea dispozitivelor mobile în spații publice trebuie făcută cu prudență pentru a elimina riscul ca informațiile afișate pe ecran să poată fi văzute de persoane neautorizate. În situația în care se poate asigura o minimă intimitate, utilizarea dispozitivelor mobile în locațiile publice trebuie restrânsă.

Pentru stocarea informațiilor cu caracter sensibil se recomandă folosirea serverelor de rețea și mai puțin a echipamentelor de tip mobil computing. Pentru a se asigura siguranța informației, discul fix al dispozitivului mobil și părțile aferente pe care se va face stocarea trebuie să fie criptate.

În funcție de arhitectura hardware și software, dispozitivele de tip mobil computing trebuie să aibă configurate soluții corespunzătoare de protecție împotriva aplicațiilor software cu potențial distructiv (viruși, spyware, malware etc.). Utilizatorul unui dispozitiv mobil trebuie să-și actualizeze permanent programele de protecție și să se asigure că folosește ultima versiune dată de producător.

Toate echipamentele mobile vor avea configurată o aplicație „screen-saver" care se va activa automat după un timp determinat de inactivitate.

Cazurile de pierdere sau furt a unui dispozitiv mobil trebuie raportate în cel mai scurt timp către managerul de departament.

Echipamentele mobile de calcul (laptop, notebook, balckberry etc.) pot conține informații cu caracter sensibil din cadrul Primăriei. În aceste condiții, utilizatorul unui astfel de dispozitiv devine responsabil pentru disponibilitatea, integritatea și confidențialitatea datelor referitoare la Primărie, pe care le are la dispoziție. Utilizarea calculatorului portabil în exteriorul Primăriei se permite doar cu acordul conducătorului și impune respectarea unor reguli:

- Utilizatorul este responsabil de supravegherea permanentă a dispozitivului.
- Utilizatorul trebuie să asigure din punct de vedere fizice securitatea echipamentului prin folosirea unor dispozitive de împiedicare a furtului (de exemplu: cablul de securitate).
- Utilizatorii trebuie să-și salveze periodic documentele pe care le dezvoltă pentru a preîntâmpina pierderea accidentală a informațiilor nesalvate.
- Pentru orice perioadă de inactivitate, dispozitivul va fi blocat, iar deblocarea se va face pe baza de parolă.
- Dispozitivele trebuie să aibă configurat un mecanism de autentificare adecvat pentru securizarea accesului.
- Este interzisă folosirea programelor software nelicențiate și instalarea aplicațiilor de către utilizatori.

Folosirea telefoanelor mobile ale Operatorului este permisă numai pentru desfășurarea convorbirilor telefonice. De asemenea, se recomandă supravegherea telefoanelor mobile, întrucât acestea ar putea conține informații din cadrul Operatorului (de exemplu, e-mail etc.).

4.4. Protecția împotriva virușilor

Operatorul are implementate măsuri de protecție ale sistemelor telefonice informatice, aplicațiilor și rețelelor și de detectare a tuturor tipurilor de viruși și a altor produse software dăunătoare.

Pe toate sistemele informatice ale Operatorului există instalate programe antivirus.

Utilizatorii au responsabilitatea de a nu modifica setările programului antivirus. Totodată, sunt responsabili de raportarea către Departamentul IT a tuturor incidentelor datorate virușilor.
Departamentul IT are următoarele responsabilități:

- să se asigure că programul antivirus este instalat pe toate stațiile utilizatorilor și pe toate serverele;
- să actualizeze definițiile virușilor;
- să înregistreze și să investigheze toate incidentele raportate de către utilizatori.

4.5. Salvarea și restaurarea datelor

Operatorul realizează salvări (backup) periodice ale sistemelor și datelor, conform procedurilor interne. Salvările sunt menținute conform prevederilor acestei norme, iar periodic sunt efectuate teste ale mediilor de stocare pentru a se verifica posibilitatea recuperării datelor în cazul unei urgențe.

LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE POLITICII ANTI-SPAM 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				