H O T Ă R Â R E

privind aprobarea Regulamentului privind protecția datelor cu caracter personal.

Consiliul local al comunei Ciulnița, întrunit în ședința ordinară din 23.09.2021.

Având în vedere:

- prevederile Regulamentului (UE) 2016/679 din 27 aprilie 2016,privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) precum și ale Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);

Examinând :

-referatul de aprobare nr. 169/13.09.2021 al primarului comunei Ciulniţa;

-raportul de specialitate nr. 170/13.09.2021 al secretarului general al comunei Ciulniţa,

-avizul nr. 137/20.09.2021 al comisiei pentru agricultura, activitati economico-financiare, servicii publice, amenajarea teritoriului si urbanism, juridica si de disciplina din cadrul consiliului local al comunei Ciulnita

-avizul nr. 138 / 20.09.2021 al comisiei pentru activităţi socio-culturale, culte, învăţământ, sănătate şi familie,protecţie copii,tineret şi sport din cadrul Consiliului local al comunei Ciulnita,

-avizul nr.139/20.09./2021 al comisiei pentru muncă şi protecţie socială, protecţie mediu şi turism din cadrul consiliului local al comunei Ciulnita,

În temeiul art.129 alin.(14), art.139 alin.(1), alin.(3), lit.a), art. 196 alin.(1), lit.a, din Ordonanța de urgență a Guvernului nr.57/2019 privind Codul administrativ, cu modificările și completările ulterioare,

H O T Ă R Ă Ş T E:

Art.1. Se aprobă Regulamentul privind protecția datelor cu caracter personal, conform anexei , care face parte integrantă din prezenta hotărâre.

Art.2. Ordonatorul principal de credite şi responsabilul cu protecția datelor cu caracter personal vor duce la îndeplinire prevederile prezentei hotărâri.

Art.3 Prevederile prezentei hotărâri vor fi aduse la cunoştinţă cetăţenilor prin grija secretarului comunei.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

NR.85

ADOPTATA LA CIULNITA
ASTĂZI 23.09.2021
Nota:prezenta hotarare a fost adoptata cu 10 voturi pentru,0 voturi impotriva (din 11 consilieri in functie,au fost prezenti 10)

Anexa la HCL nr.85/23.09.2021

REGULAMENT
privind protecța datelor cu caracter personal

CAP. 1 DISPOZIŢII GENERALE
1. 1. Obiect şi obiective

1.1.1. Prezentul regulament stabileşte normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestora;
1.1.2. Prezentul regulament asigură protecţia drepturilor şi libertăţilor fundamentale ale persoanelor fizice şi în special a dreptului acestora la protecţia datelor cu caracter personal;
1.1.3. Prezentul regulament pune accent pe transparenţa faţă de persoana vizată și responsabilizarea operatorului de date faţă de modul în care prelucrează datele cu caracter personal;

1.1.4. Exercitarea drepturilor prevăzute în prezentul regulament nu poate fi restrânsă decât în cazurile expres şi limitativ prevăzute de lege;
1.1.5. Prezentul regulament stabilește o serie de garanţii specifice pentru a proteja cât mai eficient viaţa privată a minorilor, în special în mediul on-line;

1.1.6. Libera circulaţie a datelor cu caracter personal în interiorul Uniunii Europene nu poate fi restricţionată sau interzisă din motive legate de protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

1.2. Domeniu de aplicare
1.2.1. Prezentul regulament se aplică tuturor angajaţilor Primăriei Comunei Ciulnița cu atribuţii de prelucrare a datelor cu caracter personal şi/sau după caz persoanelor împuternicite ale instituției.
1.2.2. Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

1.3. Termeni şi definiţii
În sensul prezentului regulament:
1. ***"Date cu caracter personal"*** înseamnă orice informaţii privind o persoană fizică identificată sau identificabilă ***("Persoana vizată").*** O persoana 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 identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

2."Prelucrare" înseamnă orice operaţiune sau set de operaţiuni 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* - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale şi din orice sursă;
- *înregistrarea* - consemnarea datelor cu caracter personal într-un sistem de evidenţă automat ori neautomat, care poate fi registru, fişier automat, baza de date sau orice formă de evidenţă organizată, structurată ori ad-hoc sau într-un text, înşiruire de date ori document, indiferent de modalitatea în care se înscriu datele;
- *organizarea* - ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuţiilor legale ale operatorului, în scopul eficientizării/optimizării activităţilor de prelucrare a acestora;
- *stocarea* - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranţă;
- *adaptarea* - transformarea datelor cu caracter personal colectate iniţial, conform criteriilor prestabilite şi scopurilor pentru care au fost colectate;
- *modificarea* - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menţinerii caracteristicilor de exactitate, realitate, actualitate;
- *extragerea* - scoaterea unei părţi din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat şi distinct de prelucrarea iniţială;
- *consultarea* - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operaţiuni sau set de operaţiuni de prelucrare ulterioară;
- *utilizarea* - folosirea datelor cu caracter personal, în tot sau în parte, de către şi în interiorul operatorului, împuterniciţilor operatorului ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;
- *dezvăluirea/divulgarea* - a face disponibile date cu caracter personal către terţi prin comunicare, transmitere, diseminare sau punerea la dispoziţie în orice alt mod;
- *alăturarea* - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;
- *combinarea/alinierea* - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate iniţial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;
- *blocarea* - întreruperea prelucrării datelor cu caracter personal;
- *restricţionarea* - marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
- *ştergerea* - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidenţe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistenţa, inexactitatea;
- *transformarea* - operaţiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;
- *distrugerea* - aducerea la stare de neîntrebuinţare, în condiţiile legii, definitivă şi irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

3. "Restricţionarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora și creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

4."Creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoana fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se afla persoana fizică respectivă sau deplasările acesteia;
5."Pseudonimizare/date anonime" înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri tehnice şi organizatorice care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
6. ***„Criptarea datelor"*** înseamnă un proces de codificare a datelor astfel încât să nu poată fi înțelese de către persoanele neautorizate. „Datele criptate nu mai sunt date cu caracter personal pentru cei la care ajung ilegal" (GL art. 29 – Avizul 4/2007 privind conceptul de date cu caracter personal, în ceea ce priveşte anonimizarea prin pseudonime, Aviz 05/2014 privind tehnicile de anonimizare).
Criptarea reduce riscurile, datele nu vor fi disponibile fără cheia corectă, ajută în cazul unei breșe de securitate.
7."Sistem de evidență a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;
8."Operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; dacă scopul şi mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ; operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normativ*. În sensul prezentului regulament au calitatea de Operator, Primăria Comunei Ciulnița cu toate entităţile funcţionale/structurile organizatorice – direcţii, departamente, servicii, birouri, compartimente, comisii, comitete, etc., dacă stabilesc scopul şi mijloacele de prelucrare a datelor cu caracter personal.*
9."Persoana împuternicită de operator/procesator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
10."Destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile 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 autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;
11."Parte terţă" înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
12."Consimţământ" al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
13."Încălcarea securităţii datelor cu caracter personal" înseamnă o încălcare a securităţii 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;
14."Date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;
15."Date biometrice" înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;
16."Date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;
17. „Scara largă" se referă la numărul persoanelor vizate (sau procent exact), volumul datelor, durata sau permanența activității, suprafața geografică a activității de prelucrare.
18."Întreprindere" înseamnă o persoana fizică sau juridică ce desfăşoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociaţii care desfăşoară în mod regulat o activitate economică;
19."Grup de întreprinderi" înseamnă o întreprindere care exercită controlul şi întreprinderile controlate de aceasta;
20."Reguli corporatiste obligatorii" înseamnă politicile în materie de protecţie a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce priveşte transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoana împuternicită de operator în una sau mai multe ţări terţe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;
21."Autoritate de supraveghere/ANSPDCP" înseamnă Autoritatea Naţională de Supraveghere a Datelor cu Caracter Personal;
22. „Codul numeric personal (CNP)" înseamnă un număr semnificativ care individualizează în mod unic o persoana fizică, constituind un instrument de verificare a stării civile a acesteia şi de identificare în anumite sisteme informatice de către persoanele autorizate;
23*. „Date cu caracter personal cu funcţie de identificare de aplicabilitate generală (date cu caracter special)"* înseamnă numere prin care se identifică o persoană fizică în anumite sisteme de evidenţă şi care au aplicabilitate generală, cum ar fi: codul numeric personal, seria şi numărul actului de identitate, numărul paşaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate;
24. „Utilizator" înseamnă orice persoană care acţionează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal; *are calitatea de utilizator al datelor cu caracter personal, personalul Operatorului – Primăria Comunei Ciulnița sau al împuternicitului acestuia ale cărei atribuţii de serviciu presupun operaţiuni de prelucrare a datelor cu caracter personal.*
25. „Responsabilul de protecţia datelor" înseamnă persoana din cadrul Primăriei Comunei Ciulnița cu sarcini/responsabilităţi specifice privind funcţionarea corespunzătoare a sistemului de protecţie a datelor cu caracter personal, în conformitate cu prevederile GDPR precum şi elaborarea, implementarea şi monitorizarea respectării prevederilor prezentului Regulament.

1.4. Documente de referinţă

- Regulamentul (UE) 679/2016 al Parlamentului European și al Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (GDPR);
- Legea nr. 190/2018 privind măsurile de punere în aplicare a Regulamentului (UE) 679/2018 la nivel național;
- Legislaţia internă aplicabilă în domeniul protecţiei datelor cu caracter personal;
-Decizia ANSPDCP nr. 161/2018 privind procedura de efectuare a investigațiilor;
- OUG 57/2019 privind Codul administrativ;
- Regulamentul de organizare si funcţionare;
- Regulamente și proceduri interne.

CAP.2 PRINCIPII LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL

2.1. Legalitate, echitate şi transparenţă – un principiu esenţial, strâns asociat cu drepturile fundamentale ale omului. Datele cu caracter personal trebuie să fie prelucrate ***„în mod legal, echitabil şi transparent faţă de persoana vizată.”;***

2.2. Limitări legate de scop – datele personale trebuie să fie colectate ***în scopuri bine determinate, explicite şi legitime****,* iar prelucrările ulterioare nu trebuie să se abată de la aceste scopuri. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică/ istorică ori în scopuri statistice nu se consideră incompatibilă de la scopurile iniţiale;

2.3. Minimizarea/Reducerea la minimum a datelor – orice colectare de date personale trebuie foarte bine analizată înainte de obţinerea efectivă a datelor, care trebuie să fie ***cele mai adecvate, relevante și strict limitate*** la ceea ce este absolut necesar pentru scopurile în care sunt prelucrate;

2.4. Exactitatea informaţiilor – datele cu caracter personal trebuie să fie exacte, şi, în cazul în care este necesar, trebuie să fie actualizate; operatorii trebuie să ia toate măsurile pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere;

2.5. Limitarea stocării – datele trebuie păstrate fix atât timp cât sunt necesare pentru prelucrarea asumată. Perioadele mai lungi de stocare sunt excepţii asociate cu activităţi de prelucrare în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, conform art. 89, alin.1 din GDPR, sub rezerva punerii în aplicare a măsurilor tehnice şi organizatorice adecvate prevăzute de GDPR în vederea garantării drepturilor şi libertăţilor persoanei vizate;

2.6. Integritate şi confidenţialitate – prelucrarea datelor personale trebuie făcută în cele mai adecvate condiţii de siguranţă, care să includă „protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare”.

Nerespectarea acestui principiu expune direct la breșe de securitate și confidențialitate și, implicit, la penalitățile extrem de severe prevăzute de GDPR;

2.7. Responsabilitate – ***Operatorul este responsabil de respectarea principiilor GDPR şi de a demonstra această respectare*****.** GDPR impune nu doar respectarea principiilor GDPR – de exemplu, prin documentarea deciziilor luate cu privire la o activitate de procesare, ci și să se demonstreze oricând această respectare (responsabilitate).

În consecinţă:

- Orice prelucrare de date cu caracter personal trebuie să fie legală şi echitabilă;
- Trebuie să fie transparent pentru persoanele fizice vizate că sunt colectate, utilizate, consultate sau prelucrate datele cu caracter personal care le privesc şi în ce măsură datele sunt sau vor fi prelucrate;
- Principiul transparenţei prevede că orice informaţii şi comunicări referitoare la prelucrarea respectivelor date cu caracter personal trebuie să fie uşor accesibile şi uşor de înţeles şi că trebuie să se utilizeze un limbaj simplu şi clar; acest principiu se referă în special la

informarea persoanei vizate privind identitatea operatorului şi scopurile prelucrării, precum şi la oferirea de informaţii suplimentare, pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoanele fizice vizate şi dreptul acestora de a li se confirma şi comunica datele cu caracter personal care sunt prelucrate;

- Persoanele fizice trebuie informate cu privire la riscurile, normele, garanţiile şi drepturile în materie de prelucrare a datelor cu caracter personal şi cu privire la modul în care să îşi exercite drepturile în legătură cu prelucrarea;
- Scopurile specifice în care datele cu caracter personal sunt prelucrate trebuie să fie explicite şi legitime şi să fie determinate la momentul colectării datelor respective;
- Datele cu caracter personal trebuie să fie adecvate, relevante şi limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum;
- Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace;
- Operatorul trebuie să stabilească termene pentru ștergere sau revizuirea periodică. Operatorul trebuie să ia toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse;
- Datele personale trebuie prelucrate într-un mod care să asigure în mod adecvat securitatea şi confidenţialitatea, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal şi a echipamentului utilizat pentru prelucrare.

CAP. 3 LEGALITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Prelucrarea este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele condiţii:

a) persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului;

d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este investit operatorul;

f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Nota: „Interesele legitime ale unui operator”, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terţe părţi, pot constitui un temei juridic pentru prelucrare, cu condiţia să nu prevaleze interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, luând în considerare aşteptările rezonabile ale persoanelor vizate bazate pe relaţia acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relaţie relevantă şi adecvată între persoana vizată şi operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor poate constitui un interes legitim al operatorului de date în cauză.

CAP. 4 CONSIMŢĂMÂNTUL PERSOANEI VIZATE ŞI CONDIŢIILE PRIVIND CONSIMŢĂMÂNTUL

4.1. În cazul în care prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul expres, neechivoc, liber şi informat pentru prelucrarea datelor sale cu caracter personal.

4.2. Consimțământul trebuie acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal.

4.3. În cazul în care consimţământul persoanei vizate este dat în contextul unei declaraţii scrise care se referă şi la alte aspecte, cererea privind consimţământul trebuie să fie prezentată într-o formă care o diferenţiază în mod clar de celelalte aspecte, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu.

4.4. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul trebuie dat pentru fiecare scop în parte.

4.5. Persoana vizată are dreptul să își retragă în orice moment consimţământul. Retragerea consimţământului nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca acordarea acestuia.

4.6. Atunci când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiţionată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

4.7. ***La nivelul Primăriei Comunei Ciulnița, ca Operator de date personale, consimţământul persoanelor vizate este acordat :***

- în cadrul procesului de recrutare/selecţie de personal, dacă legislația în vigoare nu prevede altfel;
- la dosarele de personal ale angajaților, pentru aspectele în care prelucrarea este legală doar prin utlilizarea consimțământului (de ex. folosirea imaginii pe site-ul și rețelele de socializare ale instituției, evenimente, serbări, situații ce nu sunt acoperite de alt temei legal);
- pentru a crea adrese de e-mail personalizate în departamentele în care se folosește comunicarea prin poșta electronică;
- în situaţia încheierii unor contracte cu partenerii de afaceri, exclusiv în situaţia în care prelucrarea datelor personale se face în scop de marketing direct (furnizarea de informaţii despre serviciile, evenimentele şi manifestările expoziţionale ale instituției);
- în situaţia abonării la newslettere (furnizarea de informaţii despre serviciile, evenimentele şi manifestările expoziţionale ale instituției);
- în situaţia înregistrării unui cont pe website-urile instituției pentru accesarea unor servicii specifice, invitarea participării specialiştilor la târguri, expoziţii şi alte asemenea evenimente (în scop de marketing direct).
- În secțiunea de „contact” aflată pe site-ul instituției;
- În situația în care se postează imagini cu persoanele fizice, prin filmări și/sau fotografii, pe site-ul și rețelele de socializare ale instituției.
- În alte situații și departamente unde prelucrarea se bazează pe consimțământ (de ex. bibliotecă, after-school, ș.a. similare)

4.8. În cadrul procesului de recrutare/selecţie de personal, Specialistul de Resurse Umane va solicita potenţialului angajat semnarea unei *Note de Informare* prin care declară că a fost informat în legătură cu prelucrarea datelor cu caracter personal la nivelul instituției, precum şi în legătură cu drepturile de care beneficiază, potrivit legislaţiei specifice. De asemenea, va solicita consimțământul acestuia pentru afișarea rezultatelor obținute în urma participării la concursul pentru ocuparea unui post vacant, dacă legislația în vigoare nu prevede altfel. Notele de

Informare și de consimțământ se vor păstra distinct în evidențele Specialistului de Resurse Umane.

4.9. În situaţia în care conducerea Primăriei decide prelucrarea în scop de marketing direct, respectiv furnizarea către partenerii contractuali a unor informaţii despre serviciile, evenimentele şi manifestările expoziţionale ale instituției etc., *entităţile funcţionale/persoanele derulatoare/responsabile de contract vor avea în vedere în mod obligatoriu exprimarea consimţământului în scopul menţionat anterior de către persoana vizată, prin bifarea unei căsuţe dedicate din contract.* Lipsa consimţământului conduce la imposibilitatea prelucrării în scop de marketing direct.

4.10. În cazul abonării la newslettere, consimţământul persoanei vizate este dat prin bifarea unei căsuţe dedicate din secţiunea website-ului, persoana fiind informată cu privire la aspectele privind protecţia datelor cu caracter personal.

4.11. În cazul înregistrării unui cont pe website-urile instituției pentru achiziţia de servicii/achitarea tarifelor online, accesarea unor servicii specifice, precum şi în cazul invitaţiilor online adresate vizitatorilor specialişti în vederea participării acestora la târguri, expoziţii şi alte asemenea evenimente etc., consimţământul persoanei vizate este dat prin bifarea unor căsuţe dedicate din secţiunea website-ului, persoana fiind informată cu privire la aspectele privind protecţia datelor cu caracter personal.

4.12. În cazul în care se postează imagini cu persoanele fizice, prin filmări și/sau fotografii, pe site-ul și rețelele de socializare ale instituției, consimțământul va fi acordat individual de către fiecare persoană în parte. În cazul minorilor sub 16 ani, consimțământul va fi acordat de titularul răspunderii părintești.

4.13. În cazul în care se postează imagini cu grupuri mari de persoane, de ex. evenimente, serbări, maratoane, târguri, expoziții etc., organizatorul evenimentului va afișa la vedere o Informare ce prevede filmarea/înregistrarea acestora, precum și detalii privind modul prin care persoanele fizice își pot exercita drepturile prevăzute de Regulamentul (UE) 679/2016 . Întrucât în aceste situații, acordarea consimțământului pentru un număr foarte mare de persoane fizice se consideră a fi un efort disproporționat, se va afișa o *Informare privind prelucrarea datelor*, cu mențiunea că orice persoană care nu dorește să apară pe înregistrări se poate adresa organizatorilor. Înainte de distribuirea imaginilor, editorii foto/video vor blura fețele persoanelor ce și-au exprimat această opțiune, astfel încât acestea să nu poată fi recunoscute/identificate, dacă nu există un alt temei legal de prelucrare a acestor date.

4.14. *Entităţile funcţionale/persoanele derulatoare/responsabile de contract, precum şi cele responsabile de operaţiunile de marketing direct (inclusiv serviciile aferente IT) vor avea în vedere în mod obligatoriu consimţământul exprimat în acest sens de către persoana vizată, pentru evitarea unor situaţii de neconformare faţă de prevederile legale privind protecţia datelor personale.*

4.15. Dacă prelucrarea datelor personale se bazează pe consimţământ, prelucrarea datelor unui copil este legală dacă acesta are cel puţin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă şi în măsura în care consimţământul respectiv este acordat sau autorizat de titularul răspunderii părinteşti asupra copilului. Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri dacă titularul răspunderii părinteşti a acordat sau a autorizat consimţământul, ţinând seama de tehnologiile disponibile. Aceste dispoziţii nu afectează dreptul general al contractelor aplicabil în statele membre UE, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

CAP. 5 REGULI SPECIALE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

5.1. Prelucrarea unor categorii speciale de date cu caracter personal

5.1.1. Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la

sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viata sexuală sau orientarea sexuală ale unei persoane fizice.

5.1.2. Prevederile anterioare nu se aplica în următoarele situaţii:

a) *când persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal* pentru unul sau mai multe scopuri specifice, cu excepţia cazului în care dreptul Uniunii sau dreptul intern prevede că interdicţia prevăzută anterior să nu poată fi ridicată prin consimţământul persoanei vizate;

b) când prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă şi al securităţii sociale şi protecţiei sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanţii adecvate pentru drepturile fundamentale şi interesele persoanei vizate;

c) când prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află in incapacitate fizică sau juridică de a-şi da consimţământul;

d) când prelucrarea este efectuată în cadrul activităţilor lor legitime şi cu garanţii adecvate de către o fundaţie, o asociaţie sau orice alt organism fără scop lucrativ şi cu specific politic, filozofic, religios sau sindical, cu condiţia ca prelucrarea să se refere numai la membrii sau la foştii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale şi că datele cu caracter personal să nu fie comunicate terţilor fără consimţământul persoanelor vizate;

e) când prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

f) când prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau ori de câte ori instanţele acţionează în exerciţiul funcţiei lor judiciare;

g) când prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate;

h) când prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacităţii de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenţă medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical şi sub rezerva respectării condiţiilor şi garanţiilor prevăzute de lege; datele cu caracter personal pot fi prelucrate în scopurile menţionate anterior în cazul în care datele respective sunt prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente.

i) când prelucrarea este necesară din motive de interes public în domeniul sănătăţii publice, cum ar fi protecţia împotriva ameninţărilor transfrontaliere grave la adresa sănătăţii sau asigurarea de standarde ridicate de calitate şi siguranţă a asistenţei medicale şi a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor persoanei vizate, în special a secretului profesional; sau

j) când prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor

şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate.

5.2. Prelucrarea datelor cu caracter personal cu funcţie de identificare generală

Datele cu caracter personal cu funcţie de identificare generală (Codul numeric personal - CNP, seria şi numărul actului de identitate/paşaportului etc.) vor fi prelucrate, exclusiv în situaţiile în care este necesară stabilirea identităţii persoanelor vizate şi prelucrarea este prevăzută în mod expres de o dispoziţie legală.

Prin legislaţia naţională se pot detalia condiţiile specifice de prelucrare a unui număr de identificare naţional sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare naţional sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanţii corespunzătoare pentru drepturile şi libertăţile persoanei vizate.

5.3. Prelucrarea datelor cu caracter personal referitoare la condamnări penale şi infracţiuni

Prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni sau la măsuri de securitate conexe se efectuează numai sub controlul unei autorităţi de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de legislaţia naţională care prevede garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorităţi de stat.

5.4. Prelucrarea care nu necesită identificarea

5.4.1. În cazul în care scopurile pentru care Primăria Comunei Ciulnița (operatorul) prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligaţia de a păstra, obţine sau prelucra informaţii suplimentare pentru a identifica persoana vizată în scopul unic al respectării legislaţiei specifice.

5.4.2. Dacă, în cazurile menţionate anterior, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, prevederile legale privind dreptul de acces, de rectificare, de ştergere, la restricţionarea prelucrării, dreptul la portabilitatea datelor nu se aplică, cu excepţia cazului în care persoana vizată, în scopul exercitării drepturilor sale menţionate anterior, oferă informaţii suplimentare care permit identificarea sa.

5.5. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video

Primăria Comunei Ciulnița, prin intermediul sistemelor de supraveghere video, prelucrează datele cu caracter personal, respectiv imaginea şi alte informaţii ce permit identificarea persoanelor vizate.

Imaginile referitoare la persoane identificate sau identificabile, prelucrate prin mijloace de supraveghere video, constituie date cu caracter personal:

a) chiar dacă nu sunt asociate cu datele de identificare ale persoanei sau

b) chiar daca nu conţin imaginea persoanei filmate, ci alte informaţii de natură să conducă la identificarea acesteia (ex: numărul de înmatriculare al vehiculului)

Scopul prelucrării datelor personale constă în: monitorizarea/securitatea persoanelor, spaţiilor şi/sau bunurilor private, prevenirea şi combaterea infracţiunilor, îndeplinirea obligaţiilor legale şi realizarea intereselor legitime.

Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se realizează numai de către persoane autorizate.

Informaţiile înregistrate sunt destinate utilizării de către Primăria Comunei Ciulnița şi pot fi comunicate numai următorilor destinatari: persoana vizată, reprezentanţii legali/împuterniciţii persoanei vizate, reprezentanţii autorizaţi ai instituției, organele de urmărire/cercetare penală, instanţe judecătoreşti, în conformitate cu prevederile legislaţiei interne şi comunitare aplicabile activităţii desfăşurate de Primărie.

Durata de stocare a datelor obţinute prin intermediul sistemului de supraveghere video este de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate. La expirarea termenului înregistrările se distrug sau se şterg.
Persoanele vizate, respectiv angajaţii, cetățenii, clienţii/potenţialii clienţi, vizitatorii şi alte persoane care intră în sediul Primăriei Comunei Ciulnița, sunt informate în legătură cu prelucrarea datelor personale prin intermediul sistemelor de supraveghere video.
Informările în cauză, precum şi indicatoarele de marcare a existenței sistemului de supraveghere video vor fi aplicate în locurile unde sunt amplasate camere de supraveghere video-CCTV. Personalul de pază/autorizat va verifica periodic starea fizică a informărilor şi a indicatoarelor anterior menţionate şi va răspunde de siguranţa şi confidenţialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video.

5.6. Prelucrarea în contextul ocupării unui loc de muncă

5.6.1. Prin lege sau prin acorduri colective, se pot prevedea norme mai detaliate pentru a asigura protecţia drepturilor şi a libertăţilor cu privire la prelucrarea datelor cu caracter personal ale angajaţilor în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligaţiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării şi organizării muncii, al egalităţii şi diversităţii la locul de muncă, al asigurării sănătăţii şi securităţii la locul de muncă, al protejării proprietăţii angajatorului sau a clientului, precum şi în scopul exercitării şi beneficierii, în mod individual sau colectiv, de drepturile şi beneficiile legate de ocuparea unui loc de muncă, precum şi pentru încetarea raporturilor de muncă.
5.6.2. Aceste norme includ măsuri corespunzătoare şi specifice pentru garantarea demnităţii umane, a intereselor legitime şi a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce priveşte transparenţa prelucrării, transferul de date cu caracter personal în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună şi sistemele de monitorizare la locul de muncă.

5.7. Prelucrarea datelor cu caracter personal în scop promoţional (marketing)

Datele cu caracter personal furnizate de persoanele vizate (cum ar fi: nume şi prenume, adresa de e-mail, nr. fax, nr. telefon mobil/fix) vor putea fi prelucrate de Primărie, doar cu consimţământul persoanelor vizate expres, neechivoc, liber, informat şi anterior exprimat, în anumite cazuri, cu respectarea drepturilor acestora, în special a dreptului de informare şi opoziţie, în următoarele scopuri: marketing (inclusiv marketing direct), concursuri, loterii publicitare, efectuarea de comunicări comerciale pentru serviciile și activitățile desfășurate, inclusiv cele dezvoltate împreună cu un partener al instituției, prin orice mijloc de comunicare, inclusiv prin intermediul serviciilor de comunicaţii electronice. Datele cu caracter personal furnizate de persoanele vizate vor putea fi folosite în scop promoţional (marketing) şi pentru produsele sau serviciile altor parteneri ai instituției, cu respectarea drepturilor persoanelor vizate.
Persoanele vizate îşi pot exercita dreptul de prevenire a unei asemenea prelucrări prin selectarea casetelor adecvate din formularele/documentele utilizate pentru colectarea datelor cu caracter personal.
Indiferent de situaţie, în cazul în care persoana vizată va dori ca datele cu caracter personal să nu mai fie prelucrate de Primărie, poate solicita în mod expres încetarea oricărei prelucrări de date. Totodată, atunci când persoana vizată doreşte să nu mai primească newslettere sau materiale informative din partea instituției, se poate dezabona folosind butonul "Dezabonare" sau „Unsubscribe”.

CAP.6 DREPTURILE PERSOANEI VIZATE ÎN CONTEXTUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

6.1. Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate

6.1.1. Primăria Comunei Ciulnița (operatorul) ia măsuri adecvate pentru a furniza persoanei vizate informaţiile legale solicitate, precum şi orice notificări şi comunicări (în situaţia exercitării drepturilor de care beneficiază potrivit legii) referitoare la prelucrare, într-o forma concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informaţiile pot fi furnizate verbal, cu condiţia ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

6.1.2. Primăria Comunei Ciulnița facilitează exercitarea drepturilor persoanei vizate.

6.1.3. ***Primăria Comunei Ciulnița furnizează persoanei vizate informaţii privind acţiunile întreprinse în urma unei cereri prin care îşi exercită drepturile de care beneficiază în baza legii, fără întârzieri nejustificate şi în orice caz în cel mult o lună de la primirea cererii.*** Această perioadă poate fi prelungită cu două luni atunci când este necesar, ţinându-se seama de complexitatea şi numărul cererilor.

6.1.4. Primăria Comunei Ciulnița informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu excepţia cazului în care persoana vizată solicită un alt format.

6.1.5. Daca nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere şi în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri şi la posibilitatea de a depune o plângere în faţa unei autorităţi de supraveghere şi de a introduce o cale de atac judiciară.

6.1.6. Informaţiile furnizate în temeiul legislaţiei specifice şi orice comunicare şi orice măsuri luate în baza exercitării drepturilor de care beneficiază, potrivit legii, persoana vizată, sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

a) fie să perceapă o taxa rezonabilă ţinând cont de costurile administrative pentru furnizarea informaţiilor sau a comunicării sau pentru luarea măsurilor solicitate;

b) fie să refuze să dea curs cererii.

În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

6.1.7. În cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea prin intermediul căreia îşi exercită drepturile de care beneficiază, potrivit legii, persoana vizată, operatorul poate solicita furnizarea de informaţii suplimentare necesare pentru a confirma identitatea persoanei vizate.

6.1.8. Informaţiile care urmează sa fie furnizate persoanelor vizate în temeiul legislaţiei specifice, pot fi furnizate în combinaţie cu pictograme standardizate pentru a oferi într-un mod uşor vizibil, inteligibil şi clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

6.1.9. *Pentru exercitarea drepturilor prevăzute de legislaţia specifică şi de prezentul Regulament, persoanele vizate se pot adresa Primăriei Comunei Ciulnița cu o cerere scrisă, datată şi semnată la adresa de corespondenţă:* ***comuna Ciulnița, str. Matei Basarab nr. 68, județul Ialomița,*** *ori la adresa de e-mail a instituției:* ***primariaciulnita@yahoo.com***

Primăria poate, dacă este cazul, să solicite persoanei vizate să pună la dispoziţie informaţii suplimentare pentru a stabili identitatea acesteia.

6.2. Dreptul la informare

6.2.1. Informaţii care se furnizează în cazul în care datele cu caracter personal sunt colectate direct de la persoana vizată

6.2.1.1. În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, Primăria, în momentul obţinerii acestor date cu caracter personal, furnizează persoanei vizate următoarele informaţii:

a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;

b) datele de contact ale responsabilului cu protecţia datelor, după caz;

c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;

d) interesele legitime urmărite de operator sau de o parte terţă, după caz;

e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

f) dacă este cazul, intenţia operatorului de a transfera date cu caracter personal în afara Spaţiului UE si al Zonei Economice Europene şi existenţa sau absenţa unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecţie sau, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

6.2.1.2. *În plus,* faţă de informaţiile menţionate anterior, în momentul în care datele cu caracter personal sunt obţinute, operatorul furnizează persoanei vizate *următoarele informaţii suplimentare* necesare pentru a asigura o prelucrare echitabilă şi transparentă:

a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

b) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;

c) atunci când prelucrarea se bazează pe consimţământul persoanei vizate, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;

d) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;

e) dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;

f) existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.2.1.3. În cazul în care operatorul intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante;

6.2.1.4. Prevederile precedente nu se aplică dacă şi în măsura în care persoana vizată deţine deja informaţiile respective.

6.2.2. Informaţii care se furnizează în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată

6.2.2.1 În cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, Primăria furnizează persoanei vizate următoarele informaţii:

a) identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;

b) datele de contact ale responsabilului cu protecţia datelor, după caz;

c) scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;

d) categoriile de date cu caracter personal vizate;

e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;

f) dacă este cazul, intenţia operatorului de a transfera date cu caracter personal în afara Spaţiului UE şi al Zonei Economice Europene şi existenţa sau absenţa unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecţie sau, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

6.2.2.2. Pe lângă informaţiile menţionate anterior, operatorul furnizează persoanei vizate următoarele informaţii necesare pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoana vizată:

a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

b) interesele legitime urmărite de operator sau de o parte terţă, după caz;

c) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării şi a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;

d) atunci când prelucrarea se bazează pe consimţământul persoanei vizate, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;

e) dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;

f) sursa din care provin datele cu caracter personal şi, dacă este cazul, dacă acestea provin din surse disponibile public;

g) existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.2.2.3. Operatorul furnizează informaţiile menţionate anterior:

a) într-un termen rezonabil după obţinerea datelor cu caracter personal, dar nu mai mare de o lună, ţinându-se seama de circumstanţele specifice în care sunt prelucrate datele cu caracter personal;

b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau

c) dacă se intenţionează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

6.2.2.4. În cazul în care operatorul intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obţinute, operatorul furnizează persoanei vizate, înainte de aceasta prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante.

6.2.2.5 Prevederile precedente nu se aplică dacă şi în măsura în care:

a) persoana vizată deţine deja informaţiile;

b) furnizarea acestor informaţii se dovedeşte a fi imposibilă sau ar implica eforturi disproporţionate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, sub rezerva condiţiilor şi a garanţiilor prevăzute de lege, sau în măsura în care obligaţia furnizării informaţiilor este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia masuri adecvate pentru a proteja drepturile, libertăţile şi interesele legitime ale persoanei vizate, inclusiv punerea informaţiilor la dispoziţia publicului;

c) obţinerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii Europene sau de dreptul intern sub incidenţa căruia intra operatorul şi care prevede masuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

d) în cazul în care datele cu caracter personal trebuie să rămână confidenţiale în temeiul unei obligaţii statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligaţii legale de a păstra secretul.

6.2.3. Informarea persoanelor vizate în contextul activităţilor specifice Primăriei

În contextul realizării atribuţiilor stabilite de lege şi desfăşurării activităţii curente a Primăriei Comunei Ciulnița, inclusiv derulării raporturilor de muncă, activităţii comerciale/contractuale şi /sau participării la târgurile, expoziţiile şi/sau alte evenimente specializate organizate în incinta/ pe raza Comunei Ciulnița, precum şi în contextul îndeplinirii obligaţiilor legale**, informarea persoanelor vizate se poate realiza, după cum urmează:**

- În cadrul procesului de recrutare/selecţie de personal, Specialistul de Resurse Umane va pune la dispoziţia potenţialului angajat o *Notă de Informare*, pe care acesta/aceasta o va citi şi o va semna şi prin care declară că a fost informat/ă în legătură cu prelucrarea datelor cu caracter personal la nivelul instituției, precum şi în legătură cu drepturile de care beneficiază, potrivit legislaţiei specifice. Notele de Informare se vor păstra distinct în evidenţele Specialistului de Resurse Umane.
- În contextul derulării raporturilor de muncă, Specialistul de Resurse Umane va pune la dispoziţia fiecărui angajat din cadrul instituției o *Notă de Informare*, pe care acesta/aceasta o va citi şi o va semna şi prin care declară că a fost informat/ă în legătură cu prelucrarea datelor cu caracter personal la nivelul instituției precum şi în legătură cu drepturile de care beneficiază, potrivit legislaţiei specifice. Notele de Informare se vor păstra distinct în evidențele Specialistului de Resurse Umane.
- Persoanele vizate, respectiv angajaţii, cetățenii, clienţii/potenţialii clienţi, vizitatorii şi alte persoane care intră în sediul Primăriei ale căror date sunt prelucrate prin intermediul sistemelor de supraveghere video sunt informate în acest sens prin intermediul afișării unor pictograme/ indicatoare de marcare a existentei sistemului de supraveghere video, precum si prin afișarea pe site-ul instituției a politicii de supraveghere prin mijloace video. Informările în cauză, precum şi indicatoarele de marcare a existentei sistemului de supraveghere video vor fi aplicate în locurile unde sunt amplasate camere de supraveghere video-CCTV. Personalul de pază/autorizat va verifica periodic starea fizică a informărilor şi a indicatoarelor anterior menţionate şi va răspunde de siguranţa şi confidenţialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video.
- Persoanele vizate, cetățenii care solicită diverse documente/informații ce presupune completarea de cereri si formulare tipizate vor fi informați pe verso sau separat prin alineate/fraze ușor de înțeles, cu privire la necesitatea colectării datelor și respectarea Regulamentului privind protecția datelor.
- În cadrul derulării activităţii comerciale/contractuale şi /sau participării la târgurile, expoziţiile şi/sau alte evenimente specializate organizate în incinta/pe raza Comunei Ciulnița**, informarea persoanelor vizate se realizează prin:**

▪ Condiţiile Generale, Tehnice şi de Participare ale instituției, care conţin prevederi referitoare la protecţia datelor personale;

▪ Formularul „Adeziune Contract” care conţine prevederi referitoare la protecţia datelor personale;

▪ Documentaţia contractuală încheiată de instituție, care conţine prevederi referitoare la protecţia datelor personale;

▪ Termenii şi Condiţiile specifice website-urilor Primăriei, care conţin prevederi referitoare la protecţia datelor personale;

▪ Website-urile Primăriei, în situaţia abonării la Newslettere, în cazul înregistrării unui cont pentru achiziţia de servicii/achitarea tarifului online, accesarea unor servicii specifice, transmiterea cererilor și obținerea diferitelor informații, precum şi în cazul invitaţiilor online adresate vizitatorilor specialişti în vederea participării acestora la târguri, expoziţii şi alte asemenea evenimente, etc.

Derulatorii de contracte ai Primăriei Comunei Ciulnița vor avea responsabilitatea/obligativitatea inserării în contractele încheiate şi gestionate de către aceştia

a clauzelor specifice cu privire la protecţia datelor cu caracter personal şi/sau cu privire la respectarea Condiţiilor Generale, Tehnice şi de Participare.

Elementele de conţinut ale Notelor de Informare, ale clauzelor contractuale şi ale celorlalte instrumente de informare referitoare la protecţia datelor personale sunt stabilite/actualizate, pe baza legislaţiei specifice, de către Responsabilul cu protecţia datelor al Primăriei Comunei Ciulnița şi aprobate în prealabil de către conducerea instituției.

6.3. Dreptul de acces al persoanei vizate

6.3.1. Persoana vizată are dreptul de a obţine din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc şi, în caz afirmativ, acces la datele respective şi la următoarele informaţii:

a) scopurile prelucrării;

b) categoriile de date cu caracter personal vizate;

c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din ţari terţe sau organizaţii internaţionale;

d) acolo unde este posibil, perioada pentru care se preconizează ca vor fi stocate datele cu caracter personal sau, daca acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioadă;

e) existenţa dreptului de a solicita operatorului rectificarea sau ştergerea datelor cu caracter personal ori restricţionarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

f) dreptul de a depune o plângere în fata unei autorităţi de supraveghere;

g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informaţii disponibile privind sursa acestora;

h) existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizata şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.3.2. În cazul în care datele cu caracter personal sunt transferate către o ţară terţă sau o organizaţie internaţională, persoana vizată are dreptul să fie informată cu privire la garanţiile adecvate, prevăzute de lege, referitoare la transfer.

6.3.3. Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxa rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic şi cu excepţia cazului în care persoana vizată solicită un alt format, informaţiile sunt furnizate într-un format electronic utilizat în mod curent.

6.3.4. Dreptul de a obţine o copie menţionată anterior nu aduce atingere drepturilor şi libertăţilor altora.

6.4. Dreptul la rectificare

Persoana vizata are dreptul de a obţine de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ţinându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obţine completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaraţii suplimentare.

6.5. Dreptul la ştergerea datelor ("dreptul de a fi uitat")

6.5.1. Persoana vizată are dreptul de a obţine din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligaţia de a şterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplica unul dintre următoarele motive:

a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

b) persoana vizata îşi retrage consimţământul pe baza căruia are loc prelucrarea, şi nu exista niciun alt temei juridic pentru prelucrarea lor;

c) persoana vizată se opune prelucrării şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau persoana vizată se opune prelucrării, în cazul prelucrării în scop de marketing direct;

d) datele cu caracter personal au fost prelucrate ilegal;

e) datele cu caracter personal trebuie şterse pentru respectarea unei obligaţii legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidenţa căruia se afla operatorul;

f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societăţii informaţionale menţionate în legislaţia specifică.

6.5.2. Alineatele anterioare nu se aplică în măsura în care prelucrarea este necesară:

a) pentru exercitarea dreptului la liberă exprimare şi la informare;

b) pentru respectarea unei obligaţii legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este investit operatorul;

c) din motive de interes public în domeniul sănătăţii publice;

d) în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în măsura în care dreptul la ştergere este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau

e) pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

6.6. Dreptul la restricţionarea prelucrării

6.6.1. Persoana vizată are dreptul de a obţine din partea operatorului restricţionarea prelucrării *în cazul în care se aplică unul din următoarele cazuri:*

a) persoana vizată contestă exactitatea datelor, pentru o perioada care îi permite operatorului să verifice exactitatea datelor;

b) prelucrarea este ilegală, iar persoana vizată se opune ştergerii datelor cu caracter personal, solicitând în schimb restricţionarea utilizării lor;

c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanţă; sau

d) persoana vizată s-a opus prelucrării, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

6.6.2. În cazul în care prelucrarea a fost restricţionată conform prevederilor anterioare, astfel de date cu caracter personal pot, cu excepţia stocării, să fie prelucrate numai cu consimţământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau pentru protecţia drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

6.6.3. O persoană vizată care a obţinut restricţionarea prelucrării este informată de către operator înainte de ridicarea restricţiei de prelucrare.

6.7. Obligaţia de notificare cu privire la rectificarea, ştergerea datelor cu caracter personal sau restricţionarea prelucrării

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ştergere a datelor cu caracter personal sau restricţionare a prelucrării, cu excepţia cazului în care acest lucru se dovedeşte imposibil sau presupune eforturi disproporţionate.

Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

6.8. Dreptul la portabilitatea datelor

6.8.1. Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

a) prelucrarea se bazează pe consimţământ sau pe un contract; şi

b) prelucrarea este efectuată prin mijloace automate.

6.8.2. În exercitarea dreptului său la portabilitatea datelor, persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

6.8.3. Exercitarea dreptului la portabilitatea datelor nu aduce atingere dreptului la ştergerea datelor. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este investit operatorul.

6.8.4. Dreptul la portabilitatea datelor nu aduce atingere drepturilor şi libertăţilor altora.

6.9. Dreptul la opoziţie şi procesul decizional individual automatizat

6.9.1. Dreptul la opoziţie

6.9.1.1. În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situaţia particulară în care se află, prelucrării datelor cu caracter personal care o privesc, inclusiv creării de profiluri. Operatorul nu mai prelucrează datele cu caracter personal, cu excepţia cazului în care operatorul demonstrează că are motive legitime şi imperioase care justifică prelucrarea şi care prevalează asupra intereselor, drepturilor şi libertăţilor persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanţă.

6.9.1.2. Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

6.9.1.3 În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

6.9.1.4. Cel târziu în momentul primei comunicări cu persoana vizată, dreptul la opoziţie menţionat este adus în mod explicit în atenţia persoanei vizate şi este prezentat în mod clar şi separat de orice alte informaţii.

6.9.1.5. În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare ştiinţifică sau istorică sau în scopuri statistice, persoana vizată, din motive legate de situaţia sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepţia cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

6.9.2. Procesul decizional automatizat, crearea de profiluri

6.9.2.1. Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

6.9.2.2. Prevederile anterioare nu se aplică în cazul în care decizia:

a) este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator de date;

b) este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate; sau

c) are la baza consimţământul explicit al persoanei vizate.

6.9.2.3. În cazurile în care decizia este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator de date sau are la bază consimţământul explicit al persoanei vizate, operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate, cel puţin dreptul acesteia de a obţine intervenţie umană din partea operatorului, de a-şi exprima punctul de vedere şi de a contesta decizia.

6.9.2.4. Deciziile menţionate anterior nu au la baza categoriile speciale de date cu caracter personal, cu excepţiile prevăzute de lege (ex: persoana vizată şi-a dat

consimţământul explicit) şi în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

6.9.3. Dreptul de a depune plângere în fața unei Autorități de Supraveghere

6.9.3.1. Plângerile către Autoritatea Națională de Supraveghere pot fi adresate de orice persoană vizată, care consideră că modul de prelucrare a datelor sale cu caracter personal încalcă prevederile legale în vigoare, în special în cazul în care reşedinţa sa obişnuită, locul său de muncă sau presupusa încălcare se află sau, după caz, are loc pe teritoriul României. Plângerea se înaintează personal sau prin reprezentant (cu anexarea împuternicirii emise în condiţiile legii de un avocat sau a procurii notariale, după caz).

6.9.3.2. Plângerile pot fi depuse la registratura generală de la sediul de corespondență al ANSPDCP: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Bld. G-ral. Gheorghe Magheru 28-30, Sector 1, cod postal 010336, București, România, sau pot fi transmise **prin poştă, inclusiv cea electronică** (anspdcp@dataprotection.ro) ori prin **utilizarea formularului electronic**, disponibil pe pagina de internet a autorității, la secțiunea *Plângeri* (https://www.dataprotection.ro/?page=Plangeri_RGPD&lang=ro)

6.9.4. Dreptul persoanei vizate de a se adresa justiției. În situația în care persoana fizică ce a depus o plângere este nemulțumită de modul de soluționare a acesteia de către ANSPDCP, se poate adresa secţiei de contencios administrativ a tribunalului competent.

CAP. 7 RESTRICŢII

Prin legislaţia specifică care se aplică operatorului de date sau persoanei împuternicite de operator se poate restricţiona domeniul de aplicare al obligaţiilor şi al drepturilor prevăzute în actuala legislaţie în măsura în care dispoziţiile acesteia corespund drepturilor şi obligaţiilor menţionate anterior, atunci când o astfel de restricţie respectă esenţa drepturilor şi libertăţilor fundamentale şi constituie o măsură necesară şi proporţională într-o societate democratică, pentru a asigura:

a.a) securitatea naţională;

a.b) apărarea;

a.c) securitatea publică;

a.d) prevenirea, investigarea, depistarea sau urmărirea penală sau executarea sancţiunilor penale, inclusiv protejarea împotriva ameninţărilor la adresa securităţii publice şi prevenirea acestora;

a.e) alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar şi fiscal şi în domeniul sănătăţii publice şi al securităţii sociale;

a.f) protejarea independenţei judiciare şi a procedurilor judiciare;

a.g) prevenirea, investigarea, depistarea şi urmărirea penală a încălcării eticii în cazul profesiilor reglementate;

a.h) funcţia de monitorizare, inspectare sau reglementare legată, chiar şi ocazional, de exercitarea autorităţii oficiale;

a.i) protecţia persoanei vizate sau a drepturilor şi libertăţilor altora;

a.j) punerea în aplicare a pretenţiilor de drept civil.

CAP. 8 OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

8.1. Responsabilitatea Operatorului

8.1.1. Ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, costurile implementării precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, **Primăria Comunei Ciulnița pune în aplicare**

măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu legislaţia specifică.
De asemenea, măsurile tehnice şi organizatorice adoptate de instituție sunt necesare protejării datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.
Pentru îndeplinirea cerinţelor legale specifice protecţiei datelor cu caracter personal Primăria Comunei Ciulnița implementează măsuri tehnice şi organizatorice orientate pe diferite direcţii de acţiune, precum: alocarea/stabilirea responsabilităţilor pentru Responsabilul de protecţia datelor, alocarea/responsabilităţilor pentru angajaţii care prelucrează date cu caracter personal, elaborarea regulamentului privind protecţia datelor, adaptarea activităţilor instituției la cerinţele legale specifice, elaborarea/implementarea unor politici/proceduri IT adecvate pentru securitatea datelor personale, instruirea personalului, monitorizarea conformităţii, etc.
8.1.2. Măsurile tehnice şi organizatorice **includ punerea în aplicare de către Primărie a unor politici/proceduri IT adecvate de protecţie/securitate a datelor cu caracter personal.**
8.1.3. Suplimentar, măsurilor anterior precizate, în vederea asigurării unui nivel adecvat de protecţie/securitate a datelor cu caracter personal, la nivelul instituției **se adoptă/stabilesc măsuri organizatorice şi reguli, precum:**
- Instalarea de sisteme de supraveghere video şi sisteme antiefracţie;
- Monitorizarea şi intervenţia în caz de alarmă asigurată în permanenţă de personal specializat/autorizat;
- Toate documentele care conţin date cu caracter personal se înregistrează şi urmează regulile de păstrare, procesare, multiplicare, transport, distrugere şi arhivare stabilite prin Legea Arhivelor Naţionale, legislaţia internă şi internaţională privind protecţia datelor cu caracter personal, şi prin proceduri interne;
- Personalul instituției este instruit în legătură cu aspectele legale privind protecţia datelor personale şi cu privire la riscurile pe care le comportă prelucrarea datelor personale;
- Conducerea Primăriei, împreună cu specialistul IT angajat/contractat, stabileşte fiecărui utilizator tipurile de acces şi operaţiunile permise acestuia, strict necesare pentru îndeplinirea atribuţiilor de serviciu;
- Utilizatorul/angajatul instituției poate prelucra date cu caracter personal doar pe perioada în care ocupă funcţia respectivă. Extinderea sau restrângerea atribuţiilor de prelucrare a datelor cu caracter personal se dispune de instituție atunci când utilizatorul/angajatul se află în una dintre următoarele situaţii:

a) la modificarea raporturilor de muncă;
b) la modificarea atribuţiilor privind prelucrarea datelor cu caracter personal, prevăzute în fişa postului.

Dreptul de acces al utilizatorului la sistemul de evidenţă a datelor cu caracter personal se suspendă pe perioada în care acesta se afla în una dintre următoarele situaţii:

a) se află în concediu fără plată, concediu medical, concediu pentru creşterea sau îngrijirea copilului minor, pentru o perioada mai mare de 3 luni;
b) se afla în concediu de maternitate sau concediu pentru incapacitate temporară de muncă;
c) urmează un curs sau o specializare cu scoatere din program, pentru o perioada mai mare de 3 luni;
d) pe perioada cercetării disciplinare, în situaţia în care faţă de utilizator se efectuează cercetări referitoare la prelucrarea datelor cu caracter personal cu încălcarea dispoziţiilor legale;
e) alte cazuri prevăzute de lege.

- Cu ocazia proiectării, întreţinerii, actualizării aplicaţiilor de gestiune a bazelor de date, se interzice accesul providerilor/programatorilor/personalului de întreţinere a sistemelor informatice la orice fel de date cu caracter personal deţinute/create/accesate de personalul din

structura respectiva a instituției. În aceste situaţii, se pun la dispoziţia providerilor/programatorilor/personalului de întreţinere numai date anonime/pseudonimizate;

- Pentru cazuri excepţionale, numai pe durata intervenţiei şi circumstanţiat limitativ la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal numai în prezenţa unui utilizator desemnat de operator, în această situaţie, răspunderea pentru păstrarea confidenţialităţii datelor aparţine persoanelor în cauză, sens în care trebuie să semneze un Angajament de confidenţialitate;
- Operaţiunile de colectare, introducere, modificare şi actualizare a datelor cu caracter personal se realizează numai de personalul anume desemnat de către conducătorii operatorului, conform actelor de reglementare internă;
- Primăria Comunei Ciulnița dispune măsurile tehnice necesare care să permită identificarea utilizatorului care a introdus, modificat sau actualizat datele cu caracter personal;
- Bazele de date cu caracter personal deţinute/create şi programele folosite de operatori/utilizatori sunt salvate, prin copii de siguranţă, la un interval de timp stabilit de conducerea instituției, în funcţie de mărimea, volumul şi importanţa acestor baze de date;
- Primăria Comunei Ciulnița desemnează/stabileşte utilizatori care să aibă atribuţii de serviciu şi executarea copiilor de siguranţă ale bazelor de date deţinute/create şi ale programelor folosite;
- Accesul în încăperile în care se află documente ce conţin date cu caracter personal şi/sau terminale de acces/echipamente care prelucrează date cu caracter personal este limitat la utilizatorii stabiliţi de conducătorii operatorului şi numai pentru îndeplinirea atribuţiilor de serviciu (acces restricţionat/controlat);
- Documentele, terminalele de acces/echipamentele care conţin date cu caracter personal vor fi ţinute/păstrate în fişete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare şi/sau în încăperi/spaţii care se pot încuia. Documentele care conţin date cu caracter personal, folosite pentru realizarea anumitor operaţiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora. Terminalele de acces/echipamentele se securizează cu parolă;
- Aplicaţiile informatice care gestionează date cu caracter personal trebuie prevăzute cu facilitatea închiderii automate a sesiunii de lucru dacă utilizatorul nu acţionează asupra datelor afişate pe ecran pe o perioadă de timp stabilită, prin proceduri de lucru/diagrame flux, în funcţie de operaţiunile care trebuie executate.
- Terminalele de acces trebuie să aibă setate funcţia de închidere automată a ecranului şi funcţia „lock screen - screen saver” la o temporizare prestabilită, prin proceduri de lucru/diagrame flux, iar dacă acest lucru nu este posibil din punct de vedere tehnic, după trecerea intervalului de timp stabilit, datele afişate trebuie ascunse sau sesiunea de lucru va fi închisă. Terminalele de acces folosite în relaţia cu publicul se poziţionează astfel încât datele afişate să fie vizualizate numai de către utilizatori;
- Accesul utilizatorilor/angajaţilor instituției la datele cu caracter personal care se regăsesc în Reţeaua Primăriei – serverele şi staţiile de lucru, se face controlat/restricţionat pe bază de user şi parolă, setate exclusiv de Biroul IT/responsabilul IT contractat, utilizatorii având drept de acces limitat, conform procedurilor interne (ex: read only, write, execute, modify, full control etc.);
- Nu este permisă scoaterea din instituţie a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD etc.) care conţin date cu caracter personal, decât cu aprobarea prealabilă a conducerii Primăriei;
- Se interzice utilizarea serviciului de e-mail în orice mod ce ar avea drept consecinţă transmiterea, distribuirea şi livrarea de mesaje nesolicitate de poştă electronică în volum mare sau de mesaje comerciale nesolicitate ("Spam"). Prin spam înţelegem trimiterea de mesaje (comerciale) nesolicitate în urma cărora se primesc plângeri din partea celor care le primesc, folosirea sau distribuirea de liste de e-mailuri care aparţin unor persoane care nu şi-au exprimat consimţământul anterior.

- Utilizatorii/angajaţii nu vor deschide email-uri de tip SPAM/Malware şi/sau orice alte comunicaţii electronice care nu au legătură cu activitatea desfăşurată în calitate de angajat. Totodată, angajaţii Primăriei nu au voie să găzduiască sau să permită găzduirea site-urilor sau informaţiilor a căror publicitate este făcuta prin emailuri SPAM. **Nerespectarea politicii anti-spam constituie abatere disciplinară şi se sancţionează potrivit Regulamentului Intern.**
- Utilizatorii/angajaţii din cadrul Primăriei care prelucrează date cu caracter personal sunt obligaţi să îşi închidă sesiunea de lucru, să blocheze ecranul terminalelor de acces atunci când părăsesc locul de muncă, iar la sfârşitul programului de lucru să închidă terminalele de acces;
- Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizaţi, şi, acolo unde echipamentul de imprimare permite, aceasta operaţiune se va realiza controlat, pe bază de parolă.

Prezentele reguli şi măsuri se completează cu prevederile politicilor şi procedurilor elaborate/implementate de instituție, reglementări interne necesare pentru asigurarea adecvată a protecţiei/securităţii datelor cu caracter personal.

8.1.4. Aderarea la coduri de conduită aprobate sau la un mecanism de certificare aprobat, menţionat de legislaţia specifică, poate fi utilizată ca element care să demonstreze respectarea obligaţiilor de către operator.

8.2. Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit

8.2.1. Având în vedere stadiul actual al tehnologiei, costurile implementării, şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare (mijloace manuale şi/sau automate - ex: sisteme de operare, servere, staţii de lucru, soluţii de securitate, de backup, de stocare, programe/soluţii software/aplicaţii IT achiziţionate sau dezvoltate in-house etc.), cât şi în cel al prelucrării în sine, pune în aplicare măsuri tehnice şi organizatorice adecvate (ex: pseudonimizarea), care sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor, precum reducerea la minimum a datelor, şi să integreze garanţiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele prezentului regulament şi a proteja drepturile persoanelor vizate.

8.2.2. Operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligaţie se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare şi accesibilităţii lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenţia persoanei, de un număr nelimitat de persoane.

8.2.3. Un mecanism de certificare aprobat menţionat de legislaţia specifică poate fi utilizat drept element care să demonstreze îndeplinirea cerinţelor prevăzute anterior.

8.3. Persoana împuternicită de Operator

8.3.1. În cazul în care prelucrarea urmează să fie realizată în numele operatorului, acesta contractează exclusiv persoane împuternicite care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în prezentul regulament şi să asigure protecţia drepturilor persoanei vizate.

8.3.2. Persoana împuternicită de operator nu recrutează o altă persoană împuternicită fără a primi în prealabil o autorizaţie scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizaţii generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecţii fată de aceste modificări.

8.3.3. Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte

obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului.

Respectivul contract sau act juridic prevede **în special** că persoana împuternicită de operator:

a) prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţara terţă sau o organizaţie internaţională, cu excepţia cazului în care aceasta obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;

c) adoptă toate masurile tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate a datelor personale corespunzător, în conformitate cu cerinţele legislaţiei specifice;

d) respectă condiţiile menţionate privind recrutarea unei alte persoane împuternicite de operator;

e) ţinând seama de natura prelucrării, oferă asistenţa operatorului prin masuri tehnice şi organizatorice adecvate, în măsură în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute de legislaţia specifică;

f) ajută operatorul să asigure respectarea obligaţiilor privind securitatea prelucrării, notificarea Autorităţii/informarea persoanei vizate în cazul încălcării securităţii datelor, evaluarea impactului asupra protecţiei datelor, consultarea prealabilă, ţinând seama de caracterul prelucrării şi informaţiile aflate la dispoziţia persoanei împuternicite de operator;

g) la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

h) pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.

i) Persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucţiune încalcă prezentul regulament sau alte dispoziţii din dreptul intern sau din dreptul Uniunii referitoare la protecţia datelor.

8.3.4. În cazul în care o persoana împuternicită de un operator recrutează o alta persoană împuternicită pentru efectuarea de activităţi de prelucrare specifice în numele operatorului, aceleaşi obligaţii privind protecţia datelor prevăzute în contractul sau în alt act juridic încheiat între operator şi persoana împuternicită de operator, astfel cum sunt prevăzute anterior, revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanţii suficiente pentru punerea în aplicare a unor masuri tehnice şi organizatorice adecvate.

În cazul în care această a doua persoană împuternicită nu îşi respecta obligaţiile privind protecţia datelor, persoana împuternicită iniţială rămâne pe deplin răspunzătoare faţă de operator în ceea ce priveşte îndeplinirea obligaţiilor persoanei împuternicite subsecvent.

8.3.5. Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, sau la un mecanism de certificare aprobat, menţionate de legislaţia specifică, poate fi utilizată ca element prin care să se demonstreze existența garanţiilor suficiente menţionate anterior.

8.3.6. Fără a aduce atingere unui contract individual încheiat între operator şi persoana împuternicită de operator, contractul sau celalalt act juridic încheiat între persoana împuternicită de operator și o altă persoană împuternicită, se poate baza, integral sau parţial, pe clauze

contractuale standard prevăzute/adoptate de Comisia Europeană/ de o autoritate de supraveghere, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul legislaţiei specifice;

8.3.7. Contractul sau celalalt act juridic menţionat anterior se formulează în scris, inclusiv în format electronic.

8.3.8. În cazul în care o persoană împuternicită de operator încalcă prezentul regulament, prin stabilirea scopurilor şi mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce priveşte prelucrarea respectivă.

8.3.9. În situaţiile în care sunt prelucrate date cu caracter personal în numele Primăriei Comunei Ciulnița de către persoane împuternicite (procesatori de date - ex: instituţii de credit, companii de asigurări, emitente de tichete de masă tipărite sau electronice, carduri beneficii salariaţi, companii de curierat etc.) derulatorii de contract ai instituției vor avea responsabilitatea/obligativitatea de a încheia cu fiecare dintre aceste persoane împuternicite Acorduri de prelucrare a datelor cu caracter personal, care vor avea în conţinut elementele prevăzute în prezentul Regulament şi legislaţia specifică, stabilite în prealabil de Responsabilul cu protecţia datelor şi aprobate de conducerea Primăriei.

8.4. Desfăşurarea activităţii de prelucrare sub autoritatea Operatorului sau a Persoanei Împuternicite de Operator

Persoana împuternicită de operator şi orice persoana care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

8.5. Evidentele activităţilor de prelucrare

8.5.1. „Toţi operatorii din sistemul public, persoanele împuternicite de operator, precum și operatorii din sistemul privat cu peste 250 de angajaţi, au obligaţia cartografierii prelucrărilor de date cu caracter personal efectuate, raportat la prevederile art. 30 din GDPR”- Ghid de lucru ANSPDCP. Organizaţiile din sistemul privat care au mai puţin de 250 de angajaţi nu au obligaţia de a ţine evidenţa prelucrării de date cu caracter personal, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, sau date cu caracter personal referitoare la condamnări penale şi infracţiuni, astfel cum sunt prevăzute în legislaţia specifică.

8.5.2. În situaţia în care, operatorul va intra sub incidenţa prevederilor anterior menţionate, acesta păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea lor. Respectiva evidenţă cuprinde următoarele informaţii:

a) numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;

b) scopurile prelucrării;

c) o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;

e) dacă este cazul, transferurile de date cu caracter personal către o ţara terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi documentaţia care dovedeşte existenta unor garanţii adecvate;

f) acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;

g) acolo unde este posibil, o descriere generală a masurilor tehnice şi organizatorice de securitate adecvate;

8.5.3. Fiecare operator şi, după caz, persoana împuternicită de operator păstrează o evidenţă a tuturor categoriilor de activităţi de prelucrare desfăşurate în numele operatorului, care cuprind:

a) numele şi datele de contact ale persoanei sau persoanelor împuternicite de operator şi ale fiecărui operator în numele căruia acţionează această persoană (aceste persoane), precum şi ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;

b) categoriile de activităţi de prelucrare desfăşurate în numele fiecărui operator;

c) dacă este cazul, transferurile de date cu caracter personal către o ţara terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi documentaţia care dovedeşte existenţa unor garanţii adecvate;

d) acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate adecvate.

8.5.4. Evidenţele menţionate anterior se formulează în scris, inclusiv în format electronic.

8.5.5. Operatorul sau persoana împuternicită de acesta, precum şi/sau al persoanei împuternicite de operator pun evidentele la dispoziţia autorităţii de supraveghere, la cererea acesteia, cu notificarea prealabila a Operatorului;

8.6. Cooperarea cu Autoritatea de supraveghere

Primăria Comunei Ciulnița, în calitate de Operator şi persoană împuternicită de operator şi, după caz, reprezentantul acestora cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor lor.

8.7. Măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal

8.7.1. Aspecte generale privind securitatea prelucrării

8.7.1.1. Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, *operatorul şi persoana împuternicită de acesta implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, **după caz:***

a) pseudonimizarea şi criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continuă ale sistemelor şi serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

d) un proces pentru testarea, evaluarea şi aprecierea periodică a eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

8.7.1.2. La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

8.7.1.3. Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat, menţionate în legislaţia specifică, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerinţelor prevăzute anterior.

8.7.1.4. Operatorul şi persoana împuternicită de acesta iau masuri pentru a asigura faptul că orice persoană fizică care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care aceasta obligaţie îi revine în temeiul dreptului Uniunii sau al dreptului intern.

8.7.2. Aspecte specifice privind securitatea prelucrării.

La nivelul Primăriei Comunei Ciulnița, în calitate de Operator de date cu caracter personal, *măsurile tehnice IT şi organizatorice menţionate în legislaţia specifică, necesare asigurării unui nivel adecvat de protecţie sunt implementate **prin:***

- **Identificarea, ca urmare a unor activităţi de audit de specialitate şi implementarea/utilizarea în activitatea instituției a unor soluţii tehnice IT adecvate, ţinând**

cont de costurile implementării, natura, domeniul de aplicare, contextul, scopurile prelucrării şi riscurile aferente, soluţii care să acopere aspecte prevăzute de legislaţia specifică, precum:

✓ Cerinţe de securitate de bază: testarea securităţii sistemului, întărirea sistemului, codificarea securizată, protecţia împotriva programelor malware;

✓ Politica privind parolele: autentificarea utilizatorului, autentificare cu doi factori;

✓ Managementul schimbării: separarea mediilor de testare, testarea schimbărilor, accesul dezvoltatorilor;

✓ Controlul accesului: controlul accesului bazat pe roluri, securitatea conturilor de utilizator, revizuirea privilegiilor, Audit logs, conturi neutilizate, privilegiile utilizatorilor tehnici, consola de securitate, informaţii despre utilizatori;

✓ Managementul evenimentelor: log format documentation, log information, log protection and monitoring, log format, evenimente auditate;

✓ Securitatea datelor: criptarea datelor, securitatea datelor în ciclul lor de viaţă;

✓ Back-up: back-up copies, programul de back-up, back-up security, verificarea back-up-urilor, viabilitatea back-up-urilor;

✓ Pseudominimizarea, minimizarea, integritatea datelor personale (computere, servere, terminale de acces, imprimarea datelor), disponibilitatea datelor, ştergerea şi portabilitatea datelor, evidenţele activităţilor de prelucrare etc.

- Elaborarea/implementarea/monitorizarea permanentă de către Primăria Comunei Ciulnița a unor politici/proceduri specifice de protecţie/securitate a datelor cu caracter personal.

8.7.3. Cartografierea datelor cu caracter personal

În vederea cartografierii datelor cu caracter personal, Responsabilul cu protecția datelor completează și actualizează datele colectate intr-un document/formular centralizator, împreună cu conducătorii/șefii de departamente, cu suportul altor funcţii implicate din cadrul instituției ori de câte ori intervin modificări cu privire la natura activităţilor desfăşurate, structura organizatorică, datele prelucrate, categoriile vizate, introducerea unor noi măsuri de securitate etc. Conducătorii/șefii de departamente sunt responsabili de corectitudinea şi completitudinea informaţiilor furnizate prin acest formular şi implicit de asigurarea implementării măsurilor de securitate la nivelul biroului, inclusiv de urmărirea ducerii la îndeplinire a Planurilor de măsuri aferente biroului/structurii de conformare cu regulamentul 2016/679 şi instruirea personalului din subordine cu privire la aplicarea legislaţiei privind protecţia datelor cu caracter personal. Formularul completat se păstrează atât în format electronic, cât şi fizic.

În cazul în care măsurile de securitate implementate nu sunt adecvate, în funcţie de riscurile asupra protecţiei datelor din punctul de vedere al persoanelor vizate, conducătorii/șefii de departamente, împreună cu Responsabilul cu Protecția Datelor, propun *Planuri de măsuri* de conformare. Pentru estimarea riscurilor se ia în considerare natura datelor, domeniul de aplicare, contextul și scopurile prelucrării și utilizarea noilor tehnologii.

8.7.4. Reguli de gestionare a bazelor de date din punct de vedere GDPR

Se interzice realizarea de comunicări comerciale în scop de marketing direct (ex. Newslettere) către persoanele vizate care se regăsesc la nivelul instituției în diverse evidențe, baze de date, aplicaţii IT, utilizând adrese de e-mail de tipul Gmail, Yahoo sau alte adrese care conţin date cu caracter personal ori numere de telefon personale (SMC) care se regăsesc în aceste evidente, în lipsa consimţământului expres, neechivoc, liber exprimat anterior dar şi informat al persoanelor vizate și evidenţiat distinct.

Comunicările comerciale în scop de marketing direct se vor putea realiza utilizând doar adrese de email create pe propriul domeniu sau alte adrese similare care conţin date cu caracter personal ori numere de telefon personale (SMC) care se regăsesc în

evidenţele, aplicaţiile, bazele de date utilizate la nivelul instituției, numai în măsura în care:

- avem consimţământul expres neechivoc, liber exprimat anterior dar şi informat al persoanelor vizate, şi
- evidenţele, aplicaţiile, bazele de date utilizate la nivelul instituției vor fi adaptate în sensul evidenţierii în mod distinct a consimţământului persoanelor vizate, pentru controlul efectiv al acestui proces d.p.d.v. GDPR, indiferent de modalitatea de obţinere a acestuia.

Datele trebuie să fie adecvate, relevante şi strict limitate la ce este absolut necesar pentru scopurile în care sunt necesare pentru prelucrarea asumată.

Fiecare conducător al locului de muncă, cu suportul Biroului/responsabilul IT, va identifica şi inventaria, menţine în reţeaua organizaţiei, inclusiv în staţiile de lucru individuale, doar bazele de date care sunt utile în mod efectiv pentru desfăşurarea activităţii curente a organizaţiei, precum şi eliminarea acelora care nu mai au relevanţă pentru activitatea Primăriei şi/sau a expirat termenul de arhivare. Lista bazelor de date gestionate de fiecare birou va conţine minim: denumirea bazei de date, locaţia de păstrare, responsabilul de gestionare (elaborare, modificare), persoanele cu drepturi de acces, perioada de păstrare, frecventa back-ul etc.

Fiecare conducător al locului de muncă care gestionează baze de date în reţeaua organizaţiei şi pe staţiile de lucru individuale, cu suportul Biroului/responsabilului IT, vor stabili reguli de acces controlat/restricţionat (ex. Read only, write, execute, modify etc.) pentru utilizatorii acestor baze de date, revizuite în sensul celor de mai sus, pe bază de user şi parola, la niveluri de acces (dacă este posibil).

Bazele de date trebuie grupate în foldere dedicate, atât a celor utilizate pentru activităţi comerciale/relaţii de afaceri cât şi a bazei de date utilizate în scop de marketing direct pentru persoane fizice.

În reţeaua instituţiei conducătorii locurilor de muncă, cu suportul Biroului/responsabilului IT, se vor menţine doar documentele care conţin date cu caracter personal care sunt relevante, utile în mod efectiv pentru desfăşurarea activităţii curente a Primăriei şi eliminarea tuturor acelora care nu au relevanţă, sau sunt documente personale.

Biroul/responsabilul IT va realiza/asigura în permanenţă, conform programelor aprobate, salvarea bazelor de date cu caracter personal precum şi a altor documente ce conţin date cu caracter personal în reţeaua instituţiei, prin copii de siguranţă (back-up), la intervalul stabilit.

8.8. Notificarea Autorităţii de Supraveghere în cazul încălcării securităţii datelor cu caracter personal

8.8.1. În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, Primăria Comunei Ciulnița, prin Responsabilul cu protecţia datelor, notifică acest lucru Autorităţii de supraveghere competente, fără întârzieri nejustificate şi, daca este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. În cazul în care notificarea Autorităţii nu are loc în termen de 72 de ore, aceasta va fi însoţită de o explicaţie motivată a întârzierii în cauză.

8.8.2. Persoana împuternicită de operator înştiinţează operatorul (informează Responsabilul cu protecţia datelor al operatorului) fără întârzieri nejustificate după ce ia la cunoştinţă de o încălcare a securităţii datelor cu caracter personal.

8.8.3. Notificarea adresată Autorităţii cu privire la încălcarea securităţii datelor personale, conţine cel puţin, următoarele elemente:

a) descrierea caracterului încălcării securităţii datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile şi numărul aproximativ al persoanelor vizate în cauză, precum şi categoriile şi numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

b) numele şi datele de contact ale responsabilului cu protecţia datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;
c) descrierea consecinţelor probabile ale încălcării securităţii datelor cu caracter personal;
d) descrierea masurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securităţii datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.
8.8.4. Atunci când şi în măsura în care nu este posibil să se furnizeze informaţiile în acelaşi timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.
8.8.5. Operatorul, prin Responsabilul cu protecţia datelor, păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse. Aceasta documentaţie permite Autorităţii de supraveghere să verifice conformitatea cu legislaţia specifică.
8.8.6. Angajaţii Primăriei Comunei Ciulnița au obligația de a informa de îndată șeful ierarhic şi Responsabilul cu protecţia datelor în cazul identificării unei situaţii de încălcare a securităţii datelor cu caracter personal.
Responsabilul cu protecţia datelor analizează informaţiile comunicate, iar dacă este cazul, solicită entităţilor funcţionale date şi informaţii suplimentare.
În cazul în care situaţia de încălcare a securităţi datelor cu caracter personal este fundamentată rezonabil, Responsabilul cu protecţia datelor întocmeşte Notificarea şi solicită avizul conducătorului instituției (Primarul) pentru a fi transmisă la Autoritatea de Supraveghere.
Notificarea se transmite către Autoritatea de Supraveghere pe suport de hârtie sau în format electronic, conform cerinţelor stabilite de Autoritate.
8.9. Informarea Persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal
8.9.1. În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul, prin Responsabilul cu protecţia datelor, informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.
8.9.2. În informarea transmisă persoanei vizate, prevăzută anterior, se include o descriere într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor cu caracter personal, precum şi cel puţin următoarele informaţii şi măsuri:
- numele şi datele de contact ale responsabilului cu protecţia datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;
- descrierea consecinţelor probabile ale încălcării securităţii datelor cu caracter personal;
- descrierea măsurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securităţii datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

8.9.3. Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiţii este îndeplinită:
a) operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată sa le acceseze, cum ar fi criptarea;
b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile şi libertăţile persoanelor vizate nu mai este susceptibil să se materializeze;
c) ar necesita un efort disproporţionat. În această situaţie, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

CAP.9 EVALUAREA IMPACTULUI ASUPRA PROTECŢIEI DATELOR ŞI CONSULTAREA PREALABILĂ

9.1. Evaluarea impactului asupra protecţiei datelor

9.1.1. Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, *în cazul în* care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul, prin Responsabilul cu protecţia datelor, efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operaţiuni de prelucrare similare care prezintă riscuri ridicate similare.

9.1.2. Responsabilul cu protecția datelor elaborează, la solicitarea operatorului, în colaborare cu angajaţii instituției, evaluarea impactului asupra unui anumit tip de prelucrare de date cu caracter personal.

9.1.3. Evaluarea impactului asupra protecției datelor se impune mai ales în cazul:

a) unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

b) prelucrării pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale şi infracţiuni menţionate în legislaţia specifică; sau

c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

9.1.4. Autoritatea de supraveghere <u>întocmeşte şi publică</u> o listă a tipurilor de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor.

9.1.5. Autoritatea de supraveghere <u>poate,</u> de asemenea, să stabilească şi să pună la dispoziţia publicului o listă a tipurilor de operaţiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecţiei datelor.

9.1.6. <u>Evaluarea conţine cel puţin:</u>

a) o descriere sistematica a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

b) o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;

c) o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate; şi

d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal şi să demonstreze conformitatea cu dispoziţiile prezentului regulament, luând în considerare drepturile şi interesele legitime ale persoanelor vizate şi ale altor persoane interesate.

9.1.7. La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite a codurilor de conduită aprobate, menţionate în legislaţia specifică, în special în vederea unei evaluări a impactului asupra protecţiei datelor.

9.1.8. Operatorul, prin Responsabilul cu protecţia datelor, <u>solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanţilor</u> acestora privind prelucrarea prevăzută, fără a aduce atingere protecţiei intereselor comerciale sau publice ori securităţii operaţiunilor de prelucrare.

9.1.10. Atunci când prelucrarea are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidenţa căruia intră operatorul, iar dreptul respectiv reglementează operaţiunea de prelucrare specifică sau setul de operaţiuni specifice în cauză şi deja s-a efectuat o evaluare a impactului asupra protecţiei datelor ca parte a unei evaluări a impactului general în contextul adoptării respectivului temei juridic, prevederile anterioare nu se aplică, cu excepţia cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfăşurării activităţilor de prelucrare.

9.1.11. Acolo unde este necesar, operatorul, prin Responsabilul cu protecţia datelor, efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecţiei datelor, cel puţin atunci când are loc o modificare a riscului reprezentat de operaţiunile de prelucrare.

9.2. Consultarea prealabila a Autorităţii de Supraveghere

9.2.a.i.1.1. Operatorul, prin Responsabilul de protecţia datelor, consultă Autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecţiei datelor indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului.

9.2.a.i.1.2. Atunci când consultă Autoritatea de supraveghere, operatorul, prin Responsabilul cu protecţia datelor, îi furnizează acesteia:

a) dacă este cazul, responsabilităţile respective ale operatorului, ale operatorilor asociaţi şi ale persoanelor împuternicite de operator implicate în activităţile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

b) scopurile şi mijloacele prelucrării preconizate;

c) măsurile şi garanţiile prevăzute pentru protecţia drepturilor şi libertăţilor persoanelor vizate, în conformitate cu prezentul regulament;

d) datele de contact ale responsabilului cu protecția datelor personale ;

e) evaluarea impactului asupra protecţiei datelor; şi

f) orice alte informaţii solicitate de Autoritatea de supraveghere.

9.2.a.i.1.3. Dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere şi să obţină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecţia socială şi sănătatea publică.

CAP.10 RESPONSABILUL DE PROTECŢIA DATELOR

10.1. Alocarea responsabilităţilor/sarcinilor aferente Responsabilului cu protecţia datelor

La nivelul Primăriei Comunei Ciulnița sarcinile/responsabilităţile Responsabilului cu protecţia datelor au fost alocate persoanei desemnate/contractate.

Responsabilităţile stabilite sunt următoarele:

- Participă la procesul de tranziţie către conformitatea cu Regulamentul privind Protecţia Datelor cu Caracter Personal (GDPR);
- informează şi consiliază Primăria Comunei Ciulnița, sau persoana împuternicită de instituție, precum şi angajaţii acesteia care se ocupă de prelucrarea datelor cu caracter personal privind obligaţiile (naţionale şi europene) referitoare la prelucrarea datelor cu caracter personal, precum şi cu privire la orice aspect legat de protecţia datelor cu caracter personal;
- acordă consiliere şi se implica în mod direct în efectuarea evaluărilor de impact asupra protecţiei datelor, monitorizează funcţionarea acestora, inclusiv privind consultarea prealabilă a autorităţii de supraveghere, dacă este cazul;
- monitorizează respectarea prevederilor legale (naţionale şi europene) şi ale reglementărilor interne referitoare la protecţia datelor personale la nivelul Primăriei;
- monitorizează alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
- participă la instruirea angajaţilor implicaţi în operaţiunile de prelucrare a datelor personale;
- participă la activitatea de actualizare a evidenţei operaţiunilor de prelucrare a datelor personale şi monitorizează corectitudinea acesteia;
- redactează şi negociază clauze contractuale privind prelucrarea datelor cu caracter personal;

- monitorizează, utilizând metoda eşantionului, modul în care persoanele ale căror date cu caracter personal se procesează, au fost informate de drepturile pe care le au;
- asigură asistenţa privind gestionarea prelucrării de date cu caracter personal, menţinerea registrului de prelucrări a datelor personale precum şi registrul privind incidentele de securitate şi efectuează notificările privind încălcarea securităţii datelor personale;
- cooperează cu Autoritatea de supraveghere (ANSPDCP) si acţionează ca punct de contact în relaţia cu autoritatea de supraveghere, persoanele vizate, precum şi în cadrul Primăriei în legătură cu aspecte de prelucrare;

10.2. Responsabilităţile Primăriei Comunei Ciulnița faţă de Responsabilul cu protecţia datelor

- Conducerea Primăriei şi conducătorii entităţilor funcţionale din cadrul instituției se vor asigură că Responsabilul cu protecţia datelor este implicat corespunzător şi în timp util în toate aspectele legate de protecţia datelor cu caracter personal;
- Conducerea Primăriei şi conducătorii entităţilor funcţionale din cadrul instituţiei vor acorda întregul sprijin Responsabilului cu protecția datelor, asigurându-i resursele necesare pentru executarea atribuţiilor sale, precum şi pentru accesarea datelor cu caracter personal şi a operaţiunilor de prelucrare şi pentru menţinerea cunoştinţelor sale de specialitate;
- Responsabilul de protecţia datelor nu va primi niciun fel de instrucţiuni în ceea ce privește îndeplinirea atribuţiilor sale în legătură cu GDPR.
- Persoanele vizate pot contacta şi solicită asistenţa de specialitate din partea Responsabilului cu protecţia datelor cu privire la toate aspectele legate de prelucrarea datelor si de exercitarea drepturilor lor;
- Conducerea Primăriei şi responsabilul cu protecţia datelor se vor asigura că niciuna din sarcinile celui din urmă nu generează un conflict de interese.

CAP.11 TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ŢĂRI TERŢE SAU ORGANIZAŢII INTERNAŢIONALE

11.1. Orice decizie de a transfera date în afara spaţiului UE şi al Zonei Economice-Europene va fi supusă, anterior transferului şi în timp util, analizei Responsabilului cu protecţia datelor.

Transferurile de date în afara spaţiului UE şi al Zonei Economice-Europene se pot face:

- În temeiul unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecţie;
- În baza unor garanţii adecvate oferite de Primărie sau persoana împuternicită a instituției.

Garanţiile adecvate pot fi furnizate prin:

a) un instrument obligatoriu d.p.d.v. juridic şi executoriu între autorităţile sau organismele publice;

b) reguli corporatiste obligatorii;

c) clauze standard de protecţie a datelor adoptate de Comisia Europeană;

d) clauze standard de protecţie a datelor adoptate de o autoritate de supraveghere şi aprobate de Comisia Europeană;

e) un cod de conduită aprobat, însoţit de un angajament obligatoriu şi executoriu din partea Primăriei sau a persoanei împuternicite de instituție din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f) un mecanism de certificare aprobat, însoţit de un angajament obligatoriu şi executoriu din partea Primăriei sau a persoanei împuternicite de instituție din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate.

11.2. Sub rezerva autorizării din partea autorităţii de supraveghere, garanţiile adecvate pot fi furnizate, în special, prin:

a) clauze contractuale între Primărie, persoana împuternicită de instituție şi operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din ţara terţă sau organizaţia internaţională; sau

b) dispoziţii care urmează să fie incluse în acordurile administrative dintre autorităţile sau organismele publice, care includ drepturi opozabile şi efective pentru persoanele vizate.

11.3. În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie sau a unor garanţii adecvate, **un transfer de date către o ţară terţă sau o organizaţie internaţională poate avea loc numai în una dintre condiţiile următoare:**

a) persoana vizată şi-a exprimat în mod explicit acordul cu privire la transfer, după ce a fost informată asupra posibilelor riscuri pe care transferurile le pot implica pentru persoana vizată;

b) transferul este necesar pentru executarea unui contract între persoana vizată şi Primărie sau pentru aplicarea unor masuri precontractuale adoptate la cererea persoanei vizate;

c) transferul este necesar pentru încheierea sau pentru executarea unui contract încheiat în interesul persoanei vizate între Primărie şi o alta persoană fizică sau juridică;

d) transferul este necesar din considerente importante de interes public;

e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanţă;

f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizica sau juridica de a-şi exprima acordul;

g) transferul se realizează dintr-un registru care, potrivit dreptului UE sau al dreptului intern, are scopul de a furniza informaţii publicului şi care poate fi consultat de public în general, sau de orice persoană care poate face dovada unui interes legitim.

11.4. In lipsa unei decizii a Comisiei, a unor garanţii adecvate dar şi în lipsa condiţiilor precizate anterior, **un transfer către o ţara terţă sau o organizaţie internaţională poate avea loc numai în cazul în care:**

- transferul nu este repetitiv;
- se referă doar la un număr limitat de persoane vizate;
- este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile şi libertăţile persoanei vizate şi
- operatorul a evaluat toate circumstanţele aferente transferului de date şi, pe baza acestei evaluări, a prezentat garanţii corespunzătoare în ceea ce priveşte protecţia datelor cu caracter personal. Operatorul informează Autoritatea de supraveghere cu privire la transfer.

CAP.12 CĂI DE ATAC, RĂSPUNDERI, MĂSURI ŞI SANCŢIUNI SPECIFICE

12.1. Dreptul de a depune o plângere la o autoritate de supraveghere

12.1.1.Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o Autoritate de supraveghere, în special în statul membru în care îşi are reşedinţa obişnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.

12.1.2. Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluţia şi rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul legislaţiei specifice.

12.2. Dreptul la o cale de atac judiciară eficientă împotriva unei Autorităţi de supraveghere

12.2.1. Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercită o cale de atac judiciară eficientă

împotriva unei decizii obligatorii din punct de vedere juridic a unei Autorităţi de supraveghere care o vizează.

12.2.2. Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere competentă nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluţionarea plângerii depuse.

12.2.3. Acţiunile introduse împotriva unei autorităţi de supraveghere sunt aduse în faţa instanţelor din statul membru în care este stabilită Autoritatea de supraveghere.

12.2.4. În cazul în care acţiunile sunt introduse împotriva unei decizii a unei Autorităţi de supraveghere care a fost precedată de un aviz sau o decizie a Comitetului european pentru protecţia datelor în cadrul mecanismului pentru asigurarea coerenţei, Autoritatea de supraveghere transmite curţii avizul respectiv sau decizia respectivă.

12.3. Dreptul la o cale de atac eficientă împotriva unui operator sau a unei persoane împuternicite de operator

12.3.1. Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o Autoritate de supraveghere, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul legii au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prevederile legale specifice.

12.3.2. Acţiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fata instanţelor din statul membru unde operatorul sau persoana împuternicită de operator îşi are un sediu. Alternativ, o astfel de acţiune poate fi prezentată în faţa instanţelor din statul membru în care persoana vizată îşi are reşedinţa obişnuită, cu excepţia cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acţionează în exercitarea competențelor sale publice.

12.4. Dreptul la despăgubiri şi răspunderea operatorului sau a persoanei împuternicite de operator

12.4.1. Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a legislaţiei specifice are dreptul să obţină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

12.4.2. Orice operator implicat în operaţiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operaţiunile sale de prelucrare care încalcă prevederile legislaţiei specifice. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligaţiile din legislaţia specifică care revin în mod specific persoanelor împuternicite de operator sau a acţionat în afara sau în contradicţie cu instrucţiunile legale/contractuale ale operatorului.

12.4.3. Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere dacă dovedeşte că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.

12.5. Condiţii generale pentru impunerea amenzilor administrative

12.5.1. Autoritatea de supraveghere asigură faptul că impunerea unor amenzi administrative pentru încălcările prevederilor legislaţiei specifice este, în fiecare caz, eficace, proporţională şi disuasivă.

12.5.2. În funcţie de circumstanţele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menţionate de legislaţia specifică.

Autoritatea poate:

- să emită avertizări;
- să emită mustrări;
- să dea dispoziţii;

- să oblige operatorul să informeze persoana vizată cu privire la o încălcare a protecţiei datelor;
- să limiteze sau să interzică prelucrarea;
- sa dispună rectificarea sau ştergerea datelor sau restricţionarea prelucrării.

În cazul în care operatorul va fi sancţionat administrativ pentru nerespectarea legislaţiei privind protecţia datelor cu caracter personal, Responsabilul cu protecţia datelor va analiza oportunitatea contestării sancţiunii administrative şi va formula propuneri în legătură cu promovarea căii de atac, precum şi, dacă este cazul, va elabora contestaţia, urmând să analizeze cel puţin următoarelor aspecte:

a) natura, gravitatea şi durata încălcării, ţinându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum şi de numărul persoanelor vizate afectate şi de nivelul prejudiciilor suferite de acestea;

b) dacă încălcarea a fost comisă intenţionat sau din neglijenţă;

c) orice acţiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;

d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice şi organizatorice implementate de aceştia;

e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;

f) gradul de cooperare cu Autoritatea de supraveghere pentru a remedia încălcarea şi a atenua posibilele efecte negative ale încălcării;

g) categoriile de date cu caracter personal afectate de încălcare;

h) modul în care încălcarea a fost adusă la cunoştinţa Autorităţii de supraveghere, în special dacă şi în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

i) în cazul în care măsurile menţionate de legislaţia specifică au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la acelaşi obiect, respectarea respectivelor măsuri;

j) aderarea la coduri de conduită sau la mecanisme de certificare aprobate; şi

k) orice alt factor agravant sau atenuant aplicabil circumstanţelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

Responsabilul cu date personale va reprezenta operatorul în cadrul procedurii administrative în fața Autorităţii cât şi în situaţia în care se va contesta decizia Autorităţii în fata instanţelor judecătoreşti.

12.5.3. Neconformarea faţă de prevederile GDPR poate atrage aplicarea de amenzi administrative cuprinse între 10.000.000 EUR şi 20.000.000 EUR sau între 2% si 4% din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul valoarea cea mai mare.

CAP.13 RESPONSABILITĂŢI ÎN CADRUL PRIMĂRIEI COMUNEI CIULNIȚA

13.1. Cunoaşterea şi aplicarea corespunzătoare a prezentului Regulament reprezintă obligaţia întregului personal al Primăriei Comunei Ciulnița potrivit limitelor de autoritate aprobate;

13.2. Responsabilităţile privind protecţia datelor cu caracter personal revin gradual întregului personal al Primăriei Comunei Ciulnița;

13.3. Responsabilităţile în ceea ce priveşte elaborarea, avizarea, aprobarea, implementarea, supravegherea şi evaluarea aplicabilităţii prezentului Regulament, precum şi dispunerea masurilor care se impun revin, după cum urmează:

13.3.1. PRIMĂRIA COMUNEI CIULNIȚA (cu toate structurile organizatorice), în calitate de Operator:

a) asigură implementarea legislaţiei comunitare-UE şi naţionale privind protecţia datelor cu caracter personal la nivelul instituției, prin prezentul regulament sau alte acte interne ;
b) asigură conformarea tuturor activităţilor de prelucrare cu prevederile legislaţiei comunitare-UE şi naţionale privind protecţia datelor cu caracter personal;
c) asigură informarea persoanelor vizate şi respectă drepturile acestora;
d) ia măsurile necesare pentru a asigura securitatea prelucrării datelor cu caracter personal;
e) asigură respectarea prezentului regulament privind masurile de protecţie a persoanelor cu privire la prelucrarea datelor cu caracter personal.
13.3.2. CONDUCEREA PRIMĂRIEI COMUNEI CIULNIȚA aprobă prezentul Regulament privind protecţia datelor cu caracter personal. Conducerea Primăriei va supraveghea implementarea Regulamentului privind protecţia datelor cu caracter personal, inclusiv prin asigurarea că problemele de conformare sunt rezolvate eficient şi prompt.
Conducerea Primăriei aprobă modificări ale prezentului Regulament, în situaţia în care schimbările legislative impun acest lucru și:
a) Participă la întocmirea Regulamentului Primăriei privind prelucrarea datelor cu caracter personal;
b) aprobă prin acte de reglementare internă/acte decizionale măsuri de implementare a prevederilor legale incidente şi ale Regulamentului privind prelucrarea datelor cu caracter personal;
c) asigură prin instrumentele de control şi/sau audit intern/extern evaluarea proceselor aferente prezentului Regulament şi aplicarea legislaţiei în domeniul protecţiei datelor;
13.3.3. Organele de Conducere ale Primăriei Comunei Ciulnița şi conducătorii structurilor sale organizatorice (direcţii, servicii, birouri, compartimente etc.) sunt responsabili cu protecţia datelor cu caracter personal pentru activităţile coordonate şi au în acest sens următoarele responsabilităţi specifice:
a) stabilesc scopul şi mijloacele de prelucrare a datelor cu caracter personal atunci când acestea sunt necesare în contextul derulării activităţii comerciale/contractuale şi/sau participării la târgurile, expoziţiile şi/sau evenimentele specializate organizate de instituție şi/sau în incinta/pe raza Orș., inclusiv desfăşurării activităţii curente a instituției, precum şi în contextul îndeplinirii obligaţiilor legale;
b) asigură elaborarea/actualizarea procedurilor proprii şi, după aprobarea acestora de către conducere le pun în aplicare;
c) asigură implementarea şi monitorizează respectarea actelor de reglementare internă şi a legislaţiei specifice, în materia prelucrării datelor cu caracter personal de către utilizatorii (angajaţii) din subordine;
d) coordonează şi monitorizează activitatea personalului pe linia protecţiei datelor cu caracter personal la nivelul operatorului;
e) asigura desfăşurarea pregătirii de specialitate şi instruirea utilizatorilor în acest domeniu;
f) dispun masuri de completare sau, după caz, de modificare a fişei posturilor utilizatorilor;
g) analizează şi dispun în ceea ce priveşte suspendarea sau revocarea dreptului de acces al utilizatorilor la sisteme de evidenţă a datelor cu caracter personal, în condiţiile legii;
h) dispun măsuri organizatorice pentru exercitarea drepturilor de către persoana vizată;
i) coordonează procesul de furnizare a datelor şi informaţiilor necesare în vederea soluţionării cererilor persoanelor vizate;
j) ţin evidenţa cererilor persoanelor vizate care au legătură cu activităţile coordonate ce implica prelucrarea datelor cu caracter personal;
k) analizează periodic activitatea utilizatorilor;
l) informează operativ Responsabilul cu protecţia datelor despre vulnerabilităţile şi riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii şi propune masuri pentru înlăturarea acestora;
m) informează operativ Responsabilul cu protecţia datelor în legătură cu orice încălcare a normelor de protecţie a datelor cu caracter personal de natură a prejudicia drepturile persoanei

vizate, cu privire la măsurile dispuse pentru identificarea persoanei responsabile şi limitarea efectelor unei diseminări neautorizate a datelor, precum şi cu privire la situaţiile în care au fost emise recomandări sau aplicate sancţiuni de către Autoritatea naţională de supraveghere sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigaţii.

13.3.4. Utilizatorii, respectiv angajaţii Primăriei care prelucrează date cu caracter personal au următoarele responsabilităţi specifice:

a) să cunoască şi să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum şi ale prezentului regulament;

b) să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condiţiile legii, cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute şi consecinţele refuzului de a le pune la dispoziţie, drepturile prevăzute de lege, condiţiile în care pot fi exercitate aceste drepturi etc.;

c) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu şi să acorde sprijin şefilor ierarhici, organelor de conducere ale Primăriei, pentru realizarea activităţilor specifice ale acestora;

d) să păstreze confidenţialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;

e) să respecte măsurile de securitate, precum şi celelalte reguli stabilite la nivelul Primăriei;

f) să informeze de îndată seful ierarhic şi Responsabilul cu protecţia datelor despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situaţie în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoştinţă.

13.3.5. Derulatorii de contracte din cadrul Primăriei

a) au responsabilitatea/obligativitatea inserării în contractele încheiate şi gestionate de către aceştia a clauzelor specifice (elaborate de/împreună cu Responsabilul cu protecţia datelor) cu privire la protecţia datelor cu caracter personal;

b) în situaţiile în care sunt prelucrate date cu caracter personal în numele Primăriei de către persoane împuternicite (procesatori de date-ex: instituţii de credit, companii de asigurări, emitente de tichete de masă tipărite sau electronice, carduri beneficii salariaţi, companii de curierat etc.) derulatorii de contract vor avea responsabilitatea/obligativitatea de încheia cu fiecare dintre aceste persoane împuternicite Acorduri de prelucrare a datelor cu caracter personal, care vor avea în conţinut elementele prevăzute în prezentul Regulament şi legislaţia specifică, stabilite în prealabil de Responsabilul cu protecţia datelor şi aprobate de conducerea Primăriei.

c) în situaţia prelucrării datelor personale în scop de marketing direct, derulatorii de contract, precum şi salariaţii responsabili de operaţiunile de marketing direct (inclusiv serviciile aferente IT) vor avea în vedere în mod obligatoriu consimţământul exprimat anterior prelucrării de către persoana vizată, pentru evitarea unor situaţii de neconformare faţă de prevederile legale privind protecţia datelor personale.

13.3.6. Responsabilul cu protecţia datelor este responsabil cu elaborarea Regulamentului şi controlul procesului, incluzând: monitorizarea si controlul aplicării unitare a Regulamentului, testarea conformităţii, audituri de specialitate şi informarea conducerii Primăriei; participă la organizarea şi administrarea programelor de pregătire continuă a angajaţilor în domeniul cunoaşterii prevederilor GDPR; responsabilităţile acestuia sunt menţionate în prezentul regulament şi/sau în contractul de prestării-servicii încheiat.

13.3.7. Specialistul Resurse Umane:

a) asigură informarea potenţialilor angajaţi şi a angajaţilor Primăriei Comunei Ciulnița cu privire la prelucrarea datelor cu caracter personal şi la drepturile de care beneficiază potrivit legii;

b) participă la organizarea şi administrarea programelor de pregătire continuă a angajaţilor în domeniul protecţiei datelor personale;
c) La angajarea salariaţilor în cadrul Primăriei, pune la dispoziţia acestora documentele necesare în vederea informării cu privire la prevederile prezentului Regulament şi se asigură de luarea la cunoștință, prin semnatură.
13.3.8. Biroul/Responsabilul IT – se asigură de:
a) luarea măsurilor tehnice şi organizatorice, specifice zonei IT, prevăzute de prezentul Regulament;
b) elaborarea/implementarea/monitorizarea permanentă a politicilor/procedurilor specifice de protecţie/securitate a datelor cu caracter personal la nivelul Primăriei.
c) instruirea utilizatorilor/angajaţilor cu privire la politicile/procedurilor specifice de protecţie/securitate a datelor cu caracter personal.
13.3.9. Conducerea societăţilor cărora le-au fost externalizate activităţi sau a agenţilor/ intermediarilor (după caz)- responsabil de proces.

CAP.14 ANGAJAMENTUL DE CONFORMARE A ANGAJAŢILOR PRIMĂRIEI FAŢĂ DE LEGISLAŢIA SPECIFICĂ ŞI REGULAMENTUL PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL

14.1. La angajare, înainte de începerea activităţilor de prelucrare a datelor cu caracter personal, dar şi ulterior, cu ocazia derulării raporturilor de muncă, organizării de instruiri profesionale specifice, toţi angajaţii care prelucrează date cu caracter personal trebuie să semneze un ***Angajament individual de conformare/Acord/o Informare*** faţă de legislaţia specifică şi a prezentului Regulament privind protecţia datelor cu caracter personal.
14.2. Confirmarea scrisă reprezintă asumarea individuală a angajamentului de respectare a legislaţiei specifice şi a Regulamentului privind protecţia datelor cu caracter personal, în scopul protejării reputaţiei Primăriei Comunei Ciulnița şi aplicării standardelor de etică.
14.3. Semnătura de confirmare înseamnă :
a) că angajatul a luat la cunoştinţă despre prevederile Regulamentului privind protecţia datelor cu caracter personal;
b) că angajatul a participat la programele de pregătire şi a fost instruit conform prevederilor Regulamentului adoptat în acest domeniu;
c) că angajatul înţelege importanţa respectării în totalitate a cerinţelor cuprinse în legislaţia specifică şi în Regulamentul privind protecţia datelor cu caracter personal;
d) că angajatul îşi asumă necondiţionat responsabilitatea în ceea ce priveşte conformarea cu cerinţele cuprinse în legislaţia specifică şi în Regulamentul privind protecţia datelor cu caracter personal;
e) că angajatul înţelege că, în situaţia nerespectării principiilor şi cerinţelor cuprinse în Regulament, se face direct răspunzător pentru încălcarea angajamentului individual şi pentru consecinţele ce decurg din acesta.
14.4. Refuzul de a semna confirmarea angajamentului individual înseamnă :
a) că este necesară identificarea motivelor reale care au condus la refuz ;
b) că este necesară instruirea suplimentară, dacă motivul real este neînţelegerea mesajului sau informaţiilor transmise ;
c) că este necesară examinarea atentă a angajatului respectiv, urmată de luarea unor masuri adecvate, mai ales în situaţia în care acesta ocupă o funcţie care prezintă un risc sensibil la adresa instituției, dacă refuzul de a semna confirmarea nu are o motivaţie reală.
14.5. Angajamentele de Conformare semnate de salariaţii Primăriei se vor păstra în evidențele Specialistului de Resurse Umane.

CAP. 15 TRAINING

15.1. Planurile anuale de pregătire continuă, elaborate în condiţiile legii, trebuie să conţină teme privind cunoaşterea legislaţiei naţionale şi comunitare în materia prelucrării datelor cu caracter personal, precum şi teme specifice privind riscurile pe care le comportă prelucrarea datelor şi măsurile minime de securitate, în funcţie de specificul activităţii instituției.
15.2. Periodic, conducătorii structurilor funcţionale din cadrul Primăriei organizează, cu sprijinul Responsabilului cu protecţia datelor, instruiri cu utilizatorii/angajaţii pentru cunoaşterea procedurilor specifice de lucru instituite la nivelul instituției şi cu privire la riscurile generate de vulnerabilităţi şi ameninţări informatice la adresa datelor cu caracter personal prelucrate.
15.3. Instruirile se efectuează periodic şi în mod obligatoriu la modificarea cadrului legal în materie, iar prelucrarea incidentelor se va realiza cu întregul personal implicat în activitatea de prelucrare a datelor cu caracter personal.

CAP.16 DISPOZIŢII FINALE

16.1. Nerespectarea prevederilor prezentului Regulament reprezintă un risc major de conformare care poate atrage pentru Primăria Comunei Ciulnița sancţiuni din partea organelor de reglementare/supraveghere competente, în condiţiile legii.
16.2. Prezentul Regulament are caracter „Uz intern”, difuzarea neautorizată a acestuia de salariaţii instituției către terţe persoane se sancţionează conform legislaţiei în vigoare.
16.3. Aplicarea sancţiunilor administrative nu înlătură răspunderea penală, civilă, materială sau contravenţională , după caz, a persoanelor vinovate.
16.4. Prezentul regulament completează: regulamentele, procedurile interne, diagramele flux, precum şi orice alte acte de reglementare internă.
16.5. Dacă ulterior datei intrării în vigoare a prezentei reglementari, o prevedere legală modifică/completează/abrogă prevederi ale prezentului regulament, se vor aplica prevederile legale în vigoare.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 1 la Regulament

Politica GENERALĂ privind protecția datelor cu caracter personal

Prezentare generală

Introducere

Primăria comunei Ciulnița prelucrează date cu caracter personal referitoare la persoane fizice. Acestea pot reprezenta date în legătură cu clienții, furnizorii, cetățenii, contacte pentru afaceri, angajați și alte persoane cu care Primăria a încheiat un contract sau cu care aceasta se află într-o legătură.
Această politică descrie modul în care datele personale trebuie colectate, utilizate și stocate pentru a fi în concordanță cu standardele instituției referitoare la protecția datelor – și, de asemenea, să îndeplinească condiția legalității.
Acest control se aplică tuturor sistemelor, persoanelor și proceselor care constituie sistemele informatice ale organizației, inclusiv membrii consiliului, directorii, angajații, furnizorii și alte părți terțe care au acces la sistemele Primăriei.

Existența politicii

Această politică privitoare la protecția datelor asigură Primăria comunei Ciulnița de:

- Conformitatea cu legislația privind protecția datelor cu caracter personal și practicile performante la acest nivel;

- Protecția drepturilor persoanelor vizate: de exemplu a partenerilor, clienților, angajaților, cetățenilor;

- Modul de stocare și prelucrare a datelor persoanelor fizice;

- Protecția instituției de posibilele riscuri referitoare la încălcarea securității datelor.

Legislația privitoare la protecția datelor cu caracter personal

Regulamentul (EU) nr. 679/2016 descrie modul în care instituțiile – incluzând Primăria comunei Ciulnița - trebuie să prelucreze datele cu caracter personal. Amenzile semnificative sunt aplicabile în cazul în care se consideră că o încălcare a fost adoptată în temeiul Regulamentului GDPR, care are rolul de a proteja datele cu caracter personal ale cetățenilor Uniunii Europene.

Aceste reguli se aplică indiferent dacă datele sunt stocate în format electronic, pe hârtie sau pe alte materiale.

Pentru a fi în concordanță cu legislația, informațiile personale trebuie să fie colectate și utilizate în mod corect, stocate în siguranță, nepermițându-se folosirea acestora în mod ilegal.

Regulamentul (EU) nr 2016/679 stipulează, printre altele, faptul că datele personale trebuie:

1. Să fie prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);

2. Să fie colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri („limitări legate de scop”);

3. Să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);

4. Să fie exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);

5. Să **nu** fie păstrate mai mult timp decât este necesar („limitări legate de stocare”);

6. Să fie prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”);

7. Să fie prelucrate în concordanță cu drepturile persoanelor vizate;

8. Să **nu** fie transferate în afara Spațiului Economic European, decât în cazul în care teritoriul/țara unde urmează a fi transferate asigură un nivel adecvat de protecție a datelor cu caracter personal.

Definiții

Există un număr total de 26 de definiții enumerate în cadrul GDPR. Definițiile cele mai fundamentale cu privire la această politică sunt următoarele:

Date cu caracter personal	orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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	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	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 dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern
Persoană împuternicită de operator	persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului

Principii privind prelucrarea datelor cu caracter personal

Există o serie de principii fundamentale pe care se bazează prelucrarea datelor personale conform Regulamentului GDPR.

Datele personale sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („**legalitate, echitate și transparență**”);

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) („**limitări legate de scop**”);

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („**reducerea la minimum a datelor**”);

(d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („**exactitate**”);

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („**limitări legate de stocare**”);

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („**integritate și confidențialitate**”).

Primăria comunei Ciulnița se va asigura că respectă toate aceste principii atât în procesul de prelucrare pe care îl desfășoară în prezent, cât și ca parte a introducerii de noi metode de procesare, cum ar fi noile sisteme informatice.

Drepturile persoanei vizate

Persoana vizată are, de asemenea, drepturi în temeiul Regulamentului GDPR. Acestea constau în:

- Dreptul de retragere a consimțământului;
- Dreptul la informare;
- Dreptul de acces;
- Dreptul la rectificare;
- Dreptul la ștergerea datelor („dreptul de a fi uitat”);
- Dreptul la restricționarea prelucrării;
- Dreptul la portabilitatea datelor;
- Dreptul de a se opune prelucrării;
- Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri;
- Dreptul de a depune o plângere la Autoritate;
- Dreptul de a se adresa justiției.

Fiecare dintre aceste drepturi este susținută de proceduri adecvate din Primăria comunei Ciulnița, care permit ca acțiunea necesară să fie luată în termenele stabilite de Regulamentul GDPR.

Persoanele vizate își pot exercita o parte din drepturile de mai sus prin e-mail sau la adresa operatorului de date (Primăriei). Operatorul de date poate atașa o cerere standard, cu toate că persoanele nu sunt obligate să o folosească.
Cererile vor fi scutite de vreo taxă. Operatorul va fi obligat să furnizeze răspuns în maxim o lună, iar în anumite cazuri excepționale în cel mult două luni de la primirea cererii.
Operatorul de date va verifica întotdeauna identitatea oricărei persoane. În vederea răspunderii la cereri și permiterea exercitării drepturilor, departamentul juridic sau consultanții juridici externi vor avea un cuvânt de spus cu privire la temeinicia cererii.
Organizația respectă următoarele termene pentru răspunsul la cererile persoanelor vizate:

Solicitarea de date solicitate	Grafic de timp
Dreptul de a fi informat	Atunci când se colectează date (dacă acestea sunt furnizate de persoana vizată) sau în termen de o lună (dacă nu sunt furnizate de persoana vizată)
Dreptul de acces	O lună
Dreptul la rectificare	O lună
Dreptul de ștergere	Fără întârzieri nejustificate
Dreptul de a restricționa procesarea	Fără întârzieri nejustificate
Dreptul la portabilitatea datelor	O lună
Dreptul de a se opune prelucrării	La primirea obiecției
Drepturi legate de procesul de luare a deciziilor și profilaxie automată.	Nespecificat

Temeiurile prelucrării

Există șase moduri alternative în care poate fi stabilită legalitatea unui caz specific de prelucrare a datelor cu caracter personal în cadrul Regulamentului GDPR.

Consimțământul

Cu excepția cazului în care este necesar dintr-un motiv admis în Regulamentul GDPR, Primăria comunei Ciulnița va obține întotdeauna acordul explicit din partea unei persoane vizate pentru colectarea și prelucrarea datelor. În cazul copiilor sub vârsta de 16 ani, va fi obținut consimțământul părinților. Informații transmise despre utilizarea datelor cu caracter personal vor fi furnizate persoanelor vizate în momentul obținerii consimțământului și explicării drepturilor acestora cu privire la datele lor, cum ar fi dreptul de retragere a consimțământului. Aceste informații vor fi furnizate într-o formă accesibilă, scrise în limbaj clar și gratuit.
În cazul în care datele cu caracter personal nu sunt obținute direct de la persoana vizată, aceste informații vor fi furnizate persoanei vizate într-o perioadă rezonabilă de timp după obținerea datelor.

Încheierea sau executarea unui contract

În cazul în care datele cu caracter personal colectate și prelucrate sunt necesare pentru a încheia sau executa un contract cu persoana vizată, nu este necesar consimțământul explicit. Acesta va fi cazul în care contractul nu poate fi încheiat fără datele personale în cauză.

Obligația legală

În cazul în care datele cu caracter personal trebuie să fie colectate și prelucrate pentru a ne conforma legii, nu este necesar consimțământul explicit. Acest lucru poate fi în cazul anumitor date referitoare la ocuparea forței de muncă și la impozitare, de exemplu.

Interesele vitale ale subiectului datelor

În cazul în care datele cu caracter personal sunt necesare pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice, atunci acesta poate fi utilizat ca temei legal al prelucrării. Primăria comunei Ciulnița va păstra dovezi rezonabile, documentate, ori de câte ori acest motiv este utilizat ca bază legală pentru prelucrarea datelor cu caracter personal.

Activitatea desfășurată în interes public

În cazul în care Primăria Comunei Ciulnița trebuie să îndeplinească o sarcină pe care o consideră a fi în interesul public sau ca parte a unei obligații oficiale, atunci nu va fi solicitat consimțământul persoanei vizate. Evaluarea interesului public va fi documentată și pusă la dispoziție ca dovezi atunci când este necesar.

Interesul legitim

Dacă prelucrarea datelor cu caracter personal specific este în interesul legitim al Primăriei comunei Ciulnița și este considerată că nu afectează în mod semnificativ drepturile și libertățile persoanei vizate, atunci aceasta poate fi definită ca fiind motivul legal al prelucrării. Din nou, raționamentul din spatele acestui punct de vedere va fi documentat.

Persoane fizice, riscuri și responsabilități

Domeniul politicii

Prezenta politică se aplică:

- Sediilor Primăriei comunei Ciulnița.
- Tuturor departamentelor Primăriei comunei Ciulnița.
- Întregului personal și voluntarilor Primăriei comunei Ciulnița.
- Tuturor contractanților, furnizorilor și altor persoane ce lucrează în numele Primăriei comunei Ciulnița.

Prezenta politică generală privind protecția datelor cu caracter personal are aplicabilitate asupra tuturor datelor pe care instituția le deține în legătură cu persoanele fizice identificabile. Acestea pot cuprinde:

- Numele persoanelor fizice;
- Adresele poștale;
- Adresele de e-mail;
- Numerele de telefon;

și orice alte date referitoare la o persoană fizică identificată sau identificabilă.

Riscurile

Politica ajută la protejarea instituției de reale riscuri la nivel de securitate, incluzând:

- Încălcări ale confidențialității.
- Vătămarea reputației. De exemplu, instituția ar putea să fie lezată dacă hackerii vor obține acces la aceste date.

Responsabilități

Oricine lucrează pentru sau cu Primăria comunei Ciulnița își angajează răspunderea pentru a asigura colectarea, stocarea și utilizarea datelor în mod corespunzător.

Fiecare echipă care utilizează datele personale trebuie să asigure faptul că acestea sunt utilizate și prelucrate în concordanță cu politica și principiile generale ale protecției datelor.

Aceste persoane au următoarele **atribuții**:

- Conducerea (Primarul) este responsabil cu privire la asigurarea îndeplinirii în mod legal a obligațiilor de către instituție.

- Responsabilul cu protecția datelor desemnat sau contractat este responsabil cu:

    - Informarea, sfătuirea angajatorului și a celorlalți angajați, emiterea de recomandări către angajator, precum și către ceilalți angajați cu privire la obligațiile care le revin în temeiul Regulamentului (EU) 2016/679 și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

    - Promovarea unei culturi a protecției datelor cu caracter personal în cadrul instituției;

    - Organizarea de training-uri în vederea pregătirii și sensibilizării angajaților cu privire la prelucrarea datelor cu caracter personal;

    - Participarea în mod regulat la ședințele conducerii, unde se iau hotărâri cu implicații privind prelucrarea datelor și oferirea de opinii concrete și documentate;

    - Colectarea informațiilor necesare pentru identificarea activităților de prelucrare;

    - Colaborarea cu celelalte departamente precum HR, Juridic, IT, pentru a avea informațiile necesare îndeplinirii sarcinilor;

    - Recomandări și sprijin concret în privința implementării cerințelor Regulamentului (EU) 2016/679, cum ar fi principiile prelucrării datelor, drepturile persoanei vizate, protecția datelor începând cu momentul conceperii și în mod implicit, păstrarea evidenței activităților de prelucrare, securitatea și managementul adecvat al incidentelor de securitate;

    - Monitorizarea respectării Regulamentului, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor;

    - Monitorizarea respectării politicilor tehnice și organizaționale ale operatorului;

    - Monitorizarea efectuării auditurilor necesare;

    - Alocarea responsabilităților, sensibilizarea și formarea personalului implicat în operațiunile de prelucrare;

    - Informarea instituției, dacă este obligatorie sau necesară efectuarea unei evaluări de impact privind protecția datelor cu caracter personal, potrivit art. (35) din Regulament;

    - Recomandări concrete în privința metodologiei care trebuie urmată pentru efectuarea unei evaluări de impact;

- În situația în care organizația nu dispune de resursele necesare pentru efectuarea internă a evaluării de impact, va recomanda externalizarea acestui proces și va îndruma organizația în alegerea corectă a persoanelor specializate care pot efectua evaluarea de impact;

- Recomandarea măsurilor care trebuie implementate (inclusiv politici tehnice și organizatorice) pentru a atenua orice riscuri la adresa drepturilor și intereselor persoanelor vizate;

- Sprijinirea conceperii și actualizării constante a evidenței activităților de prelucrare, potrivit art. (30) din Regulament;

- Cooperarea cu Autoritatea de Supraveghere;

- Asumarea rolului de punct de contact pentru Autoritatea de Supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menţionată la articolul 36, precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune;

- Asumarea rolului de punct de contact cu persoanele vizate privind toate chestiunile legate de prelucrarea datelor şi la exercitarea drepturilor în temeiul Regulamentului;

- Oferirea de sprijin concret în situația unui incident de securitate și oferirea de sprijin cu privire la notificarea Autorității/Autorităților de Supraveghere competentă/competente și a persoanelor vizate;

- Respectarea secretului și a confidențialității în ceea ce privește îndeplinirea sarcinilor sale;

- Monitorizarea și oferirea de sprijin concret în orice alt aspect legat de protecția datelor cu caracter personal, conform dispozițiilor legale în vigoare.

❖ Managerul/Responsabilul IT răspunde pentru:

- Asigurarea tuturor sistemelor, serviciilor și echipamentului folosit pentru a stoca datele, în condițiile unor standarde adecvate de securitate, asigurând confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

- Efectuarea verificărilor și scanărilor în mod constant pentru a asigura nivelul înalt de securitate al hardware-ului și software-ului, precum și funcționarea decentă a lor;

- Evaluarea fiecărui serviciu al terțului pe care instituția consideră că utilizează sau stochează date. De exemplu, servicii de cloud computing.

- Implementează măsuri pentru pseudonimizarea și criptarea datelor cu caracter personal;

- Implementează măsuri pentru a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

Regulamentul general al personalului

- ➔ Singurele persoane care sunt apte să acceseze datele prezentate în această politică trebuie să fie cele cărora le este necesară pentru activitatea pe care o realizează.

- ➔ Datele nu trebuie să fie împărtășite către toți angajații. Când este necesar accesul la informații confidențiale, angajații le pot solicita direct de la managerii/șefii lor.

- ➔ Primăria comunei Ciulnița va asigura trainingul aferent tuturor angajaților pentru a-i ajuta în procesul înțelegerii responsabilității pe care o au în momentul în care utilizează datele.

- ➔ Angajații trebuie să asigure securitatea datelor luând precauții și folosind instrucțiunile de mai jos.

- ➔ Vor trebui utilizate parole puternice.

- ➔ Datele personale nu vor fi dezvăluite către persoane neautorizate, fie din interiorul instituției sau în afară.

- ➔ Datele trebuie să fie revizuite și actualizate dacă există situația în care datele nu sunt concordante cu realitatea. Dacă nu mai sunt necesare, datele vor fi șterse.

- ➔ Angajații vor cere ajutorul managerului/superiorului lor sau responsabilului cu protecția datelor dacă nu sunt siguri în legătura cu orice aspect al protecției datelor.

Stocarea datelor

Aceste reguli descriu cum și unde ar trebui să fie stocate datele cu caracter personal. Întrebările despre stocarea datelor pot fi redirecționate în siguranță responsabilului IT sau operatorului de date.

Când datele sunt **stocate** pe **hârtie**, ele trebuie păstrate într-un loc sigur unde persoanele neautorizate nu pot avea acces.

Aceste instrucțiuni se aplică, de asemenea, asupra datelor care sunt stocate în mod obișnuit în format electronic, dar au fost printate din anumite considerente:

- Hârtiile sau fișierele trebuie păstrate într-un loc închis sau într-un sertar închis;

- Angajații trebuie să se asigure că hârtia sau cele printate nu sunt lăsate la vedere către oameni neautorizați, ca de exemplu pe imprimantă;

- Printurile trebuie distruse când nu mai sunt necesare.

Când datele sunt **stocate** în **format electronic**, ele trebuie să fie protejate de accesul neautorizat, ștergerile accidentale sau atacurilor intenționate de hacking:

- Datele trebuie protejate de parole puternice ce sunt schimbate regulat și niciodată împărtășite între angajați;

- Dacă datele sunt stocate pe suporturi amovibile (precum CD, DVD), acestea trebuie păstrate în siguranță atunci când nu sunt folosite;

- Datele trebuie stocate numai în servere sau unități specializate și trebuie să fie încărcate într-un serviciu de cloud computing aprobat;

- Serverele ce conțin informații personale trebuie plasate într-un loc sigur, departe de spațiul general de birouri;

- Datele nu trebuie salvate direct pe laptopuri sau alte dispozitive mobile precum tablete sau smartphone-uri.

- Datele trebuie să aibă un back-up. Aceste backup-uri trebuie testate regulat.

- Toate serverele și calculatoarele ce conțin date trebuie protejate de software de Securitate și firewall.

Utilizarea datelor

Datele personale nu au nicio valoare pentru Primăria comunei Ciulnița decât dacă aceasta le poate folosi în activitatea sa. Se întâmplă atunci când datele sunt accesate și folosite, iar acest fapt poate fi predispus la numeroase riscuri, corupție sau chiar furt:

- Când se lucrează cu date personale, angajații trebuie să asigure ecranele calculatoarelor întotdeauna închise când le lasă nesupravegheate;

- Datele personale nu trebuie transmite prin e-mail, având în vedere că aceasta cale de comunicare nu este sigură.

- Datele trebuie criptate înainte de a fi transferate electronic. Managerul IT trebuie să explice cum sunt trimise datele către contactele externe autorizate.

- Datele personale nu se vor transfera în afara Spațiului Economic European.

- Angajații nu trebuie să salveze datele în dispozitivele lor personale. Întotdeauna trebuie să existe acces și actualizare a copiei centrale a tuturor datelor.

Precizia datelor

Legislația solicită Primăriei comunei Ciulnița să urmărească pașii în mod rezonabil pentru a asigura precizia și actualitatea datelor. Acuratețea datelor este foarte importantă și este necesar un efort considerabil din partea instituției pentru a o asigura. Este responsabilitatea tuturor angajaților care lucrează cu aceste date să urmărească pașii pentru a asigura acuratețea și actualitatea datelor pe cât posibil.

- Datele vor fi păstrate în puține locuri. Personalul nu trebuie să creeze alte locuri adiționale deloc necesare, ca de exemplu copii inutile;

- Personalul trebuie să se folosească de fiecare oportunitate pentru a asigura actualizarea datelor.

- Primăria comunei Ciulnița va depune toate diligențele necesare pentru ca subiectele datelor să își poată actualiza informațiile pe care instituția le deține. De exemplu, prin intermediul site-ului web;

- Datele trebuie actualizate când se descoperă inadvertențe. De exemplu, când o persoana nu mai poate fi contactat prin intermediul unui număr de telefon, se recomandă eliminarea din baza de date a acestuia.

Divulgarea datelor din alte motive

În anumite circumstanțe, legislația permite datelor personale să fie dezvăluite către organele legii fără consimțământul persoanei subiect al datelor.
În aceste circumstanțe, Primăria Comunei Ciulnița va dezvălui datele necesare.
Operatorul de date va asigura faptul că cererea este legitimă, căutând asistență de la consilierii juridici ai companiei unde este necesar.

Furnizare informații

Primăria comunei Ciulnița țintește spre a asigura faptul că persoanele vizate știu cum sunt prelucrate datele, asigurându-se că ei înțeleg:

- Cum sunt datele lor utilizate;
- Cum își pot exercita drepturile.

În acest scop, instituția are o Politică de confidențialitate, stabilind cum datele sunt utilizate în cadrul acesteia.

Consecințe

Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse, ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), Primăria comunei Ciulnița va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.
Prezenta Politică va fi adusă de către conducerea instituției la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 2 la Regulament

Procedura de notificare privind confidențialitatea

Introducere
Această procedură trebuie să fie folosită atunci când este pus în aplicare sau schimbat un proces de afaceri nou care necesită colectarea de date cu caracter personal de la persoanele vizate, care intră sub incidența Regulamentului GDPR.
Regulamentul GDPR, în principal în articolele 13 și 14, solicită furnizarea de informații specifice în momentul colectării sau primirii datelor, care informează persoana vizată cu privire la utilizarea datelor și drepturile acesteia asupra acestor date. Aceste informații vor varia în funcție de circumstanțele specifice și această procedură ar trebui utilizată pentru a se asigura că informațiile corecte sunt furnizate în formatul corect, astfel încât Primăria Comunei Ciulnița să rămână în permanență compatibilă cu GDPR.
În timp ce, în trecut, informații privind confidențialitatea au fost furnizate într-un document unic (denumit adesea ,,***Politica de confidențialitate***"), GDPR se pretează mai mult la o abordare în care se utilizează notificări individuale de confidențialitate în funcție de operațiunea implicată. Acest lucru permite ca informațiile furnizate privind confidențialitatea să fie mai transparente și mai puțin confuze pentru persoana vizată.
Procedura de notificare privind confidențialitatea
Scopul acestei proceduri este de a crea o notificare adecvată privind confidențialitatea care să furnizeze persoanei vizate informațiile pe care trebuie să le primească, într-un mod cât mai corect și mai transparent posibil.
Există două modalități principale de obținere a datelor personale care sunt acoperite de Regulamentul GDPR. Acestea sunt:

- În cazul în care datele cu caracter personal sunt colectate de la persoana vizată (**articolul 13 din Regulamentul GDPR**)

- În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată (**articolul 14 din Regulamentul GDPR**)

În ambele cazuri, Regulamentul GDPR specifică informațiile care trebuie furnizate persoanei vizate. Această procedură descrie aceste informații și explică modul de creare a unui anunț de confidențialitate care să respecte cerințele Regulamentului GDPR.

Persoana vizată deține deja informațiile

Regulamentul GDPR cere ca persoana vizată să primească informațiile care se prelucrează și o vizează, cu excepția cazului în care persoana vizată deține deja informațiile. Prin urmare, este important să se stabilească dacă este rezonabil să se creadă că persoana vizată știe deja de informațiile care sunt prelucrate pe seama ei și care sunt ulterior prelucrate.

În acest caz, rațiunea pentru această credință trebuie să fie documentată și păstrată ca dovadă a conformității cu Regulamentul GDPR. Ar trebui să se acorde atenție faptului că acest lucru se aplică tuturor informațiilor solicitate și tuturor persoanelor vizate afectate, altfel ar trebui luate măsuri pentru a remedia lacunele.

În cazul în care datele cu caracter personal sunt colectate de la persoana vizată

În cazul în care persoana vizată nu deține informațiile necesare, în momentul obținerii datelor cu caracter personal trebuie să îi fie furnizate următoarele informații:

1.1..a.i.1. Identitatea și datele de contact ale operatorului și, după caz, ale persoanei împuternicite

1.1..a.i.2. Detaliile de contact ale responsabilului cu protecția datelor, după caz

1.1..a.i.3. Scopurile și temeiul juridic al procesării (de exemplu, consimțământul, obligația legală, interesul legitim)

1.1..a.i.4. Interesele legitime urmărite de către operator sau de către un terț (în cazul în care interesul legitim este definit ca fiind temeiul legal al prelucrării)

1.1..a.i.5. Destinatarii, sau categoriile de destinatari, pentru datele personale, dacă există.

1.1..a.i.6. Detalii privind orice transfer planificat de date cu caracter personal către o țară terță sau o organizație internațională

1.1..a.i.7. Durata de timp pentru care vor fi stocate datele cu caracter personal (sau criteriile utilizate pentru stabilirea acestei perioade)

1.1..a.i.8. Dreptul la accesul, rectificarea, ștergerea și transferul datelor personale ale persoanei vizate (în funcție de baza legală utilizată)

1.1..a.i.9. Dreptul persoanei vizate de a restricționa sau de a se opune vis-à-vis de prelucrarea datelor sale cu caracter personal

1.1..a.i.10. Dreptul persoanei vizate de a-și retrage consimțământul în orice moment (dacă consimțământul este utilizat ca temei legal al prelucrării)

1.1..a.i.11. Dreptul persoanei vizate de a depune o plângere la o autoritate de supraveghere

1.1..a.i.12. Dacă colectarea datelor cu caracter personal este o cerință legală sau contractuală și dacă acestea sunt obligate să le furnizeze

1.1..a.i.13. Dacă datele personale vor face obiectul unei prelucrări automate, inclusiv al profilării și, dacă da, al logicii și al posibilelor consecințe implicate

Trebuie să se acorde atenție explicării drepturilor persoanelor vizate în contextul bazei legale a prelucrării. De exemplu, dacă baza legală este un contract, atunci nu se aplică dreptul de retragere a consimțământului.

În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată

În cazul în care datele cu caracter personal nu sunt obținute direct de la persoana vizată, există o serie de circumstanțe suplimentare (adică, în plus față de cazul în care persoana vizată deține deja informațiile) admise de Regulamentul GDPR, ceea ce înseamnă că informațiile nu trebuie furnizate. Acestea sunt:

- Dacă furnizarea informațiilor se dovedește imposibilă sau ar presupune un efort disproporționat

- În cazul în care este acoperită de alte legi aplicabile care prevăd măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate (**articolul 14 din GDPR**)

- În cazul în care datele sunt confidențiale conform legii

În cazul în care se aplică oricare dintre condiții, rațiunea pentru acest aspect trebuie să fie documentată și păstrată ca dovadă a conformității cu Regulamentul GDPR. Ar trebui să se acorde atenție faptului că acest lucru se aplică tuturor informațiilor solicitate și tuturor persoanelor vizate afectate, altfel ar trebui luate măsuri pentru a remedia lacunele.

În cazul în care nu se aplică niciuna dintre aceste condiții, informațiile trebuie furnizate persoanei vizate:

- într-un termen rezonabil, cel târziu la o lună de la obținerea acesteia

- dacă este utilizat pentru comunicare (de exemplu, adrese de e-mail), cel mai târziu când are loc prima comunicare

- la punctul în care datele personale sunt comunicate unui alt destinatar (dacă este cazul)

Informațiile care trebuie furnizate sunt următoarele:

1. Identitatea și datele de contact ale operatorului și, după caz, ale persoanei împuternicite

2. Detaliile de contact ale responsabilului cu protecția datelor, după caz

3. Scopurile și temeiul juridic al prelucrării (de exemplu, consimțământul, obligația legală, interesul legitim)

4. Categoriile de date cu caracter personal, în cauză

5. Destinatarii, sau categoriile de destinatari, ale datelor personale, dacă există

6. Detalii privind orice transfer planificat de date cu caracter personal către o a treia țară sau o organizație internațională

7. Durata de timp pentru care vor fi stocate datele cu caracter personal (sau criteriile utilizate pentru stabilirea acestei perioade)

8. 8. Dreptul la accesul, rectificarea, ștergerea și transferul datelor personale ale persoanei vizate (în funcție de baza legală utilizată, a se vedea mai jos)

9. Dreptul persoanei vizate de a restricționa sau de a se opune prelucrării datelor sale personale

10. Dreptul persoanei vizate de a-și retrage consimțământul în orice moment (dacă consimțământul este utilizat ca bază legală a prelucrării)

11. Dreptul persoanei vizate de a depune o plângere la o autoritate de supraveghere

12. Originea datelor cu caracter personal

13. Dacă datele personale vor face obiectul unei prelucrări automate, inclusiv al profilării și, dacă da, al logicii și al posibilelor consecințe implicate

În ceea ce privește momentul obținerii datelor cu caracter personal direct de la persoana vizată, drepturile persoanelor vizate vor depinde de baza legală a prelucrării.

Informarea persoanei vizate

Există două formulare de planificare a notificării de confidențialitate disponibile:
(a) una care trebuie utilizată atunci când datele cu caracter personal sunt colectate direct de la persoana vizată, iar
(b) cealaltă în cazul în care datele cu caracter personal sunt obținute dintr-o altă sursă.
Utilizați formularul necesar pentru a vă asigura că toate informațiile necesare au fost completate înainte de a fi introduse în formatul adecvat pentru comunicare către persoana vizată.
Ca și în cazul tuturor informațiilor furnizate persoanelor vizate în conformitate cu Regulamentul GDPR, informațiile trebuie să fie într-o formă inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu. Cea mai bună metodă de furnizare a informațiilor către persoana vizată va depinde de specificul activității și poate include una sau mai multe dintre:

- Un anunț pe un site web
- Prin email
- Prin poștă
- Prin telefon
- Față în față

Abordarea privind notificările legate de confidențialitate trebuie planificată cu atenție, astfel încât informațiile relevante să fie prezentate persoanei vizate la momentul potrivit. Aceasta va însemna că este necesar un set coerent de anunțuri de confidențialitate, mai degrabă, decât un singur document care să acopere toată prelucrarea. Fiecare notificare privind confidențialitatea trebuie concepută astfel încât să fie afișată în momentul corespunzător al procesului de afaceri și să fie specifică informațiilor colectate, scopului pentru care vor fi puse și temeiului legal al prelucrării implicate.
În mod similar, trebuie identificat cel mai bun mod de prezentare a informațiilor. Prezentarea unui link către documentul relevant cu notificările privind confidențialitatea poate îndeplini cerințele Regulamentului GDPR pe un site web, dar metode alternative de prezentare pot permite o experiență mai ușoară a utilizatorului.

Prelucrarea ulterioară

în cazul în care se decide utilizarea datelor cu caracter personal într-un alt scop decât cel pentru care au fost obținute sau colectate datele, se pot obține informații suplimentare cu privire la acest scop, în baza considerată legală.

PREŞEDINTE DE ŞEDINŢĂ, Contrasemnează,

Fieraru Ion-Albert Pt.Secretar general al comunei,

Chițu Nela

Anexa 3 la Regulament

Politica privind facilitarea exercitării drepturilor persoanelor vizate

Introducere

Această procedură este destinată utilizării de către Primăria Comunei Ciulnița atunci când o persoană vizată exercită unul sau mai multe drepturi în temeiul Regulamentului (UE) 679/2016 (Regulamentul GDPR).

Fiecare dintre drepturile implicate are propriile sale aspecte și provocări specifice. Cu toate acestea, drepturile nu sunt absolute și există excepții. În toate cazurile, Primăria va decide dacă o cerere este întemeiată prin studierea Regulamentului GDPR. În unele cazuri, pentru a stabili dacă o cerere este întemeiată sau nu, se vor consulta departamentul juridic al insituției sau consultanții juridici externi. Răspunsul la cererea persoanei vizate se va face în termen de o lună. Dacă cererea este întemeiată, se va facilita exercitarea drepturilor. Dacă cererea nu este întemeiată, se va comunica motivul refuzului persoanei vizate și i se va comunica dreptul de a depune o plângere la ANSPDCP și dreptul de a se adresa justiției.

Dreptul de retragere a consimțământului

Persoana vizată are dreptul de a retrage consimțământul în cazul în care baza pentru prelucrarea datelor sale cu caracter personal este cea a consimțământului (adică prelucrarea nu se bazează pe alt temei legal, precum contractul, obligația legală, interesul legitim, interesele vitale sau interesul public). În multe cazuri, acordarea și retragerea consimțământului vor fi disponibile pe cale electronică, adică on-line sau in format hârtie.

În cazul în care consimțământul implică un copil (definit de GDPR ca persoana sub 16 ani) acordarea sau retragerea trebuie să fie autorizată de titularul răspunderii părintești asupra copilului.

Dreptul la informare

În momentul în care datele cu caracter personal sunt colectate de la persoana vizată sau obținute dintr-o altă sursă, există o cerință de a informa persoana vizată cu privire la utilizarea acestor date și a drepturilor asupra acestora.

Dreptul de acces

Persoana vizată are dreptul să solicite instituției o confirmare dacă datele personale sunt prelucrate, iar în caz afirmativ, are dreptul de a obține o copie a acestor date, precum și următoarele informații:

- Scopurile prelucrării;
- Categoriile datelor cu caracter personal în cauză;
- Destinatarii sau categoriile de destinatari ai datelor, dacă există, în special orice țări terțe sau organizații internaționale;

- Durata de stocare a datelor cu caracter personal (sau criteriile utilizate pentru stabilirea acestei perioade);

- Drepturile persoanei vizate la rectificarea sau ștergerea datelor sale cu caracter personal și restricționarea sau opoziția față de prelucrare;

- Dreptul persoanei vizate de a depune o plângere la o autoritate de supraveghere;

- Informații privind sursa datelor, dacă nu provin direct de la persoana vizată;

- Dacă datele personale vor face obiectul unor decizii automate, inclusiv crearea de profiluri și, dacă da, logica acestei decizii sau profilări și eventualele consecințe implicate;

- În cazul în care datele sunt transferate unei țări terțe sau unei organizații internaționale, informații privind garanțiile care se aplică;

În cele mai multe cazuri, va trebui să dam acces persoanei la date, cu excepția situației când cererea este vădit nefondată sau excesivă.

Dreptul la rectificare

În cazul în care datele cu caracter personal sunt inexacte, persoana vizată are dreptul să solicite corectarea și completarea datelor personale incomplete pe baza informațiilor pe care le furnizează.

Dacă este necesar, instituția va lua măsuri suplimentare pentru a verifica dacă informațiile furnizate de persoană sunt corecte înainte de a opera modificarea.

Dreptul la ștergere („dreptul de a fi uitat")

Persoana vizată are dreptul să solicite instituției să șteargă fără întârziere datele cu caracter personal care o privesc în următoarele cazuri:

- datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

- persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare;

- persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea

- datele cu caracter personal au fost prelucrate ilegal;

- datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;

- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale copiilor.

- Instituția va trebui să ia o decizie cu privire la o astfel de solicitare. Ștergerea datelor **nu se va realiza** dacă:

- datele sunt necesare pentru exercitarea dreptului la liberă exprimare și informare;

- datele sunt necesare pentru îndeplinirea unei obligații legale;

- din motive de interes public în domeniul sănătății publice;

- în scopuri de arhivare în interes public;
- pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Dreptul la restricționarea prelucrării

Persoana vizată își poate exercita dreptul la restricționarea prelucrării în următoarele situații:

- persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
- prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
- operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță; sau
- persoana vizată s-a opus prelucrării în conformitate cu articolul 21 alineatul (1) din Regulamentul GDPR, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

Insituția, în situația în care primește o cerere de restricționare, va trebui să verifice dacă cererea de încadrează într-unul din cazurile de mai sus. Pentru a se lua o decizie potrivită, este recomandat să se apeleze la Responsabilul cu protecția datelor ori la departamentul juridic sau consilierii legali ai instituției. În cazul în care se vor restricționa datele, acestea vor rămâne stocate, dar nu pot fi prelucrate fără consimțământul persoanei. Ele vor putea fi prelucrate pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru. În toate cazurile, persoana vizată care a obținut restricționarea prelucrării este informată de către operator înainte de ridicarea restricției de prelucrare.

Dreptul la portabilitatea datelor

Persoana vizată are dreptul să solicite ca datele personale să fie furnizate într-un format "*structurat, utilizat în mod obișnuit și care poate fi citit de mașină*" (articolul 20 din Regulamentul GDPR) și să transfere datele respective unei alte părți, de exemplu alt furnizor de servicii. Aceasta se aplică datelor cu caracter personal pentru care prelucrarea se bazează pe consimțământul persoanei vizate, pe temeiul legal al contractului sau în situația în care prelucrarea este efectuată prin mijloace automate. Acolo unde este posibil din punct de vedere tehnic, persoana vizată poate, de asemenea, solicita ca datele personale să fie transferate direct de la un operator la altul.

Dreptul la opoziție

Persoana vizată are dreptul de a se opune prelucrării care se bazează pe interesul legitim al operatorului sau al unei terțe părți sau interesul public.

Odată ce obiecția a fost făcută, insituția trebuie să justifice motivele pe care se bazează prelucrarea și să suspende prelucrarea până când decizia a fost luată. Instituția nu mai prelucrează datele cu caracter personal, cu excepția cazului în care demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea,

exercitarea sau apărarea unui drept în instanță. În cazul în care datele cu caracter personal sunt utilizate pentru marketingul direct, insituția va înceta prelucrarea.

Drepturi în legătură cu deciziile automate, inclusiv crearea profilurilor
Persoana vizată are dreptul să nu facă obiectul unei decizii automate, inclusiv crearea de profiluri în cazul în care decizia are un efect semnificativ sau juridic asupra acesteia. Persoana vizată are, de asemenea, dreptul de a-și exprima punctul de vedere, de a solicita intervenție umană și de a contesta decizia.
Există excepții de la acest drept, care sunt în cazul în care decizia:

1. Este necesară pentru încheierea sau executarea contractului;

2. Este autorizată prin lege națională sau europeană;

3. Se bazează pe consimțământul explicit al persoanei vizate;

În situațiile de la punctele (1) și (2) de mai sus, instituția va pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia. Pentru a evalua temeinicia unei astfel de cereri, insituția va trebui să decidă dacă excepțiile de mai sus se vor aplica situației. Pentru a se lua o decizie potrivită, este recomandat să se apeleze la Responsabilul cu protecția datelor ori la departamentul juridic sau consilierii legali.

Consecințe
Nerespectarea prezentei Politici de către angajații insituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici. Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 4 la rgeulament

Politica privind stocarea și protejarea înregistrărilor

Introducere
În operațiunile sale zilnice, Primăria Comunei Ciulnița colectează și stochează înregistrări de mai multe tipuri și într-o varietate de formate diferite. Fiecare tip de informație este sensibilă și importantă în felul lui, în funcție de ierarhia oferită de către

instituție prin politicile sale interne.
Este important ca aceste înregistrări să fie protejate împotriva pierderii, distrugerii, falsificării, accesului neautorizat și eliberării neautorizate, iar o serie de măsuri să fie utilizate pentru a asigura acest lucru, inclusiv copii de siguranță, control acces și criptare.
Primăria Comunei Ciulnița are, de asemenea, responsabilitatea de a se asigura că respectă toate cerințele legale, de reglementare și contractuale relevante privind colectarea, stocarea, recuperarea și distrugerea înregistrărilor. De o importanță deosebită este Regulamentul GDPR și cerințele acestuia privind stocarea și prelucrarea datelor cu caracter personal. Acest control se aplică tuturor sistemelor, persoanelor și proceselor care constituie sistemele informatice ale instituției, inclusiv membrii consiliului, directorii, angajații, furnizorii și alte părți terțe care au acces la sistemele Primăriei.

Politica privind păstrarea și protecția înregistrărilor
Politica are două componente principale:
(a) stabilirea principiilor fundamentale care trebuie adoptate atunci când se ia în considerare păstrarea, și
(b) modul în care se realizează protecția înregistrărilor.
Ulterior vor fi analizate tipurile de înregistrări deținute de Primăria Comunei Ciulnița și cerințele stabilite pentru fiecare tip de înregistrare în parte. De asemenea, vor fi abordate punctual protecția, distrugerea și gestionarea înregistrărilor.

Principii generale
Există o serie de principii generale care trebuie implementate atunci când se ia în considerare politica de păstrare și protecție a înregistrărilor. Acestea sunt:

- Înregistrările trebuie să fie ținute în conformitate cu toate cerințele legale aplicabile
- Înregistrările nu trebuie păstrate mai mult decât este necesar
- Protecția înregistrărilor în ceea ce privește confidențialitatea, integritatea și disponibilitatea lor - acestea trebuie să fie în conformitate cu cerințele de securitate
- Înregistrările trebuie să poată fi recuperabile în orice moment, dacă se poate
- Dacă este cazul, înregistrările care conțin date cu caracter personal trebuie supuse, cât mai curând posibil, analizelor privind protecția datelor cu caracter personal și cerințelor GDPR

Tipuri de înregistrări
Pentru a implementa anumite îndrumări pentru păstrare și protecție, înregistrările deținute de Primăria Comunei Ciulnița sunt grupate în categoriile enumerate în Registrul de Evidență al Prelucrării Datelor cu Carater Personal (Cartografierea datelor). Pentru fiecare dintre aceste categorii este indicată și perioadă de păstrare recomandată, mediile de stocare admise, precum și recomandări sau alte cerințe. Acestea sunt doar orientări și pot exista circumstanțe specifice în care înregistrările trebuie să fie păstrate pentru o perioadă mai lungă sau mai scurtă de timp. Aceasta va fi decisă de la caz la caz, ca parte a proiectării elementelor de securitate în cadrul instituției sau prin raportare la cerințele legale.

Utilizarea criptografiei
Dacă este cazul, pentru clasificarea informațiilor și a mediului de stocare, trebuie utilizate tehnici criptografice pentru a asigura confidențialitatea și integritatea înregistrărilor.

Trebuie să se țină seama de faptul că respectivele chei de criptare utilizate pentru criptarea înregistrărilor vor fi stocate în siguranță pentru durata de viață a înregistrărilor relevante și respectă politica instituției în domeniul criptografiei.

Selectarea mediilor de stocare

Alegerea mediilor de stocare pe termen lung trebuie să țină seama de caracteristicile fizice ale mediului de stocare, durata de utilizare, precum și de datele ce urmează să fie stocate.

În cazul în care înregistrările sunt obligatorii din punct de vedere legal să fie stocate pe hârtie, trebuie luate măsuri de precauție adecvate pentru a se asigura că condițiile de mediu rămân adecvate tipului de hârtie utilizat (*spre exemplu mediu la o anumită umiditate, dulapuri de metal securizate, care să reziste la foc etc.*). Atunci când este posibil, copiile de rezervă ale acestor înregistrări ar trebui să fie făcute prin scanare. De asemenea, trebuie să se efectueze controale regulate pentru a evalua rata de deteriorare a documentului și acțiunile întreprinse pentru păstrarea înregistrărilor, dacă este necesar.

Pentru înregistrările stocate pe suporturi electronice, cum ar fi banda, hard-drive etc. trebuie luate măsuri de precauție similare pentru a asigura longevitatea materialelor din care sunt făcute aceste suporturi, inclusiv o soluție de back-up la ele (*cum ar fi hard-drive-urile în sistem de back-up de tip mirror raid, copie de back-up de 1:1*).. Abilitatea de a citi conținutul unui anumit format de bandă (sau alt suport similar) trebuie menținută prin păstrarea unui dispozitiv capabil să îl proceseze. Dacă acest lucru nu este posibil, o terță parte externă poate fi angajată pentru a transforma mediul de stocare într-un format alternativ.

Recuperarea înregistrărilor

Este foarte important ca înregistrările să poată fi recuperate, în special în cazurile în care avem obligații legale sau comerciale. Trebuie alese soluții de o asemenea manieră încât să permită accesarea înregistrărilor într-o perioadă de timp acceptabilă, totodată prin raportare la costul stocării și viteza de recuperare.

Distrugerea înregistrărilor

Odată ce înregistrările au ajuns la sfârșitul vieții lor în conformitate cu politica internă definită și cu legilsația in vigoare, acestea trebuie să fie distruse în siguranță într-o manieră care să asigure că nu mai pot fi folosite. Procedura de distrugere trebuie să permită înregistrarea corectă a detaliilor de distrugere care ar trebui păstrate ca probă.

Revizuirea înregistrărilor

Reținerea și stocarea înregistrărilor trebuie să facă obiectul unui proces de revizuire periodic efectuat sub îndrumarea conducerii, pentru a se asigura că:

- Politica privind păstrarea și protecția înregistrărilor rămâne valabilă
- Înregistrările sunt păstrate conform politicii
- Înregistrările sunt eliminate în siguranță atunci când nu mai sunt necesare
- Sunt îndeplinite cerințele legale
- Procesele de recuperare a înregistrărilor îndeplinesc cerințele organizației

Rezultatele acestor evaluări trebuie înregistrate separat și păstrate ca dovadă.

PREŞEDINTE DE ŞEDINŢĂ, Contrasemnează,

Fieraru Ion-Albert Pt.Secretar general al comunei,

Chițu Nela

Anexa 5 la Regulament

Politica privind gestionarea datelor cu caracter personal

Introducere

Instituția va depune toate eforturile pentru a asigura securitatea și gestionarea corectă a datelor cu caracter personal pe care le prelucrează, indiferent de mediul de stocare.

Este responsabilitatea atât a conducerii instituției, cât și a oricărui angajat sau colaborator extern să se asigure că datele sunt prelucrate în condiții de siguranță potrivit Politicii de Securitate și să se asigure că nicio persoană neautorizată nu are acces la datele cu caracter personal.

Orice breșă de securitate asupra datelor cu caracter personal poate avea consecințe nefaste asupra drepturilor persoanelor, precum și prejudicii majore de imagine a companiei.

Oricine are acces la datele cu caracter personal ale instituției trebuie să știe, să înțeleagă și să adere la principiile și regulile enunțate prin prezenta Politică.

Principiile prelucrării datelor cu caracter personal

Datele cu caracter personal trebuie:

1. Să fie prelucrate în mod legal, echitabil și transparent față de persoana *vizată („legalitate, echitate și transparență”);*

2. Să fie colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri *(„limitări legate de scop”);*

3. Să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate *(„reducerea la minimum a datelor”);*

4. Să fie exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere *(„exactitate”);*

5. Să nu fie păstrate mai mult timp decât este necesar *(„limitări legate de stocare”);*

6. Să fie prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare *(„integritate și confidențialitate”);*

7. Să fie prelucrate în concordanță cu drepturile persoanelor vizate;

8. Să nu fie transferate în afara Spațiului Economic European, decât în cazul în care teritoriul/țara unde urmează a fi transferate asigură un nivel adecvat de protecție a datelor

cu caracter personal sau există un alt temei legal pentru transfer sau vreo derogare specifică.

Stocarea și accesul la datele cu caracter personal

Instituția se va asigura că sistemele informatice sunt protejate de acces neautorizat. Toți utilizatorii vor primi parole puternice care sunt schimbate periodic. Datele cu caracter personal vor fi criptate și, în măsura în care este fezabil din punct de vedere tehnic, vor fi pseudonimizate. Numele de utilizator și parolele nu vor fi niciodată împărtășite. Datele cu caracter personal pot fi accesate numai pe sisteme informatice care au parole securizate. Sistemul se va bloca automat dacă nu este utilizat timp de 5 minute.

Toate mediile de stocare a datelor cu caracter personal vor fi ținute în condiții adecvate și sigure pentru a evita furtul, pierderea sau degradarea electronică. Atunci când datele sunt stocate pe dispozitive portabile (laptop, telefon, stick, hard-disk etc), dispozitivul va fi protejat printr-o parolă puternică, iar odată ce perioada de stocare s-a terminat, datele vor fi șterse definitiv.

Datele cu caracter personal vor fi transmise către terți (de exemplu autorități ale statutului, persoane juridice – colaboratori externi) numai atunci când acest lucru este conform legii și, în toate cazurile, cu respectarea drepturilor persoanei vizate.

Consecințe

Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 6 la Regulament

Politica privind păstrarea datelor cu caracter personal

Introducere

Necesitatea de a păstra datele cu caracter personal variază foarte mult în funcție de tipul de date. Unele date pot fi șterse imediat, iar altele trebuie păstrate pentru îndeplinirea scopurilor sau pe perioada impusă de lege.

Deoarece păstrarea datelor poate fi relativă, prezenta politică este necesară astfel încât liniile directoare privind retenția datelor să fie menținute în timp în cadrul instituției.

Scop

Scopul acestei politici este de a specifica liniile directoare ale instituției pentru păstrarea diferitelor tipuri de date.

Domeniul de aplicare

Această Politică va acoperi toate datele cu caracter personal prelucrate de instituție, indiferent de mediul de stocare. În unele cazuri, perioada de stocare este impusă de lege, cum este cazul documentelor contabile (care se păstrează 10 ani), contractelor de muncă (75 de ani) sau statelor de plată (50 de ani). Retenția datelor se va realiza în conformitate cu dispozițiile legale naționale și europene privind protecția datelor cu caracter personal și, în special, în conformitate cu Regulamentul (UE) 679/2016 privind protecția datelor cu caracter personal și libera circulație a acestor date. Dacă dispozițiile prezentei Politici intră în conflict cu reglementările în materie de protecție a datelor, se vor aplica, cu prioritate, acestea din urmă.

Motive pentru a stoca datele

Instituția nu are o abordare „*Păstrăm totul*”. Acest lucru nu este nici practic, nici lipsit de costuri și nici nu respectă principiul limitării legate de stocare, enunțat de Regulamentul (UE) 679/2016. Cu toate acestea, unele date cu caracter personal vor fi păstrate, printre

altele, pentru că ne obligă legea sau pentru a ne proteja interesele comerciale. Printre motive, enumerăm:

- Litigii;
- Respectarea legii;
- Protejarea proprietății intelectuale;
- Protejarea secretelor comerciale;
- Ancheta privind incidentele de securitate.

Copiile datelor

Această Politică se aplică oricăror copii ale documentelor care conțin date cu caracter personal.

Perioada de stocare

- ***Datele cu caracter personal ale clienților***: conform Nomenclatorului Arhivistic. Ulterior acestei perioade, datele vor fi șterse total sau anonimizate complet pentru a fi utilizate în scopuri istorice, statistice sau de cercetare.
- ***Datele cu caracter personal ale candidaților la un loc de muncă:*** conform Nomenclatorului Arhivistic. Ulterior acestei perioade, datele vor fi șterse total sau anonimizate complet pentru a fi utilizate în scopuri istorice, statistice sau de cercetare.
- ***Datele cu caracter personal ale angajaților:*** conform Nomenclatorului Arhivistic. Ulterior acestei perioade, datele vor fi șterse total sau anonimizate complet pentru a fi utilizate în scopuri istorice, statistice sau de cercetare.
- ***Documentele contabile:*** conform Nomenclatorului Arhivistic. Ulterior acestei perioade, datele vor fi șterse total sau anonimizate complet pentru a fi utilizate în scopuri istorice, statistice sau de cercetare.
- ***Date ale partenerilor de afaceri sau colaboratorilor externi:*** conform Nomenclatorului Arhivistic. Ulterior acestei perioade, datele vor fi șterse total sau anonimizate complet pentru a fi utilizate în scopuri istorice, statistice sau de cercetare.
- ***Datele prelucrate pentru marketing direct***: până la retragerea consimțământului.
- ***Alte date cu caracter personal*** se vor păstra pe perioada impusă de lege, iar în lipsa acesteia pe o perioadă de 5 ani de la ultima interacțiune de orice fel cu persoana vizată.

Distrugerea datelor

La expirarea perioadei de stocare se vor distruge complet toate documentele (fizice sau electronice) care conțin date cu caracter personal prin utilizarea tehnologiei disponibile în viitor pentru documentele electronice sau prin metode fizice (distrugătoare, ardere) pentru documentele fizice. În aceeași măsură, datele pot fi anonimizate complet pentru a fi utilizate în scopuri istorice, statistice sau de cercetare.

Consecințe

Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici.

Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.
Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 7 la Regulament

Politica privind accesul la date

Scopul
Scopul acestei politici este de a menține un nivel adecvat de securitate pentru a proteja datele cu caracter personal ale Primăriei Comunei Ciulnița și sistemele de informații de acces neautorizat. Această politică definește regulile necesare pentru a asigura această protecție și pentru a asigura o funcționare sigură și fiabilă a sistemelor informatice ale instituției.
Politica
Numai utilizatorii autorizați au acces la sistemele informatice, aceștia fiind limitați la aplicații specifice, documentate și aprobate, cu diferite niveluri de acces. Accesul la sistemul informatic se realizează pe baza unui ID unic pentru fiecare utilizator.

Cui se aplică politica?

Această politică se aplică tuturor angajaților Primăriei Comunei Ciulnița și instituțiilor din grup, precum și tuturor contractanților, consultanților, angajaților temporari și partenerilor.

Angajații care încalcă în mod deliberat această politică vor fi supuși acțiunilor disciplinare prevăzute de Codul Muncii.

Sistemele afectate

Această politică se aplică tuturor calculatoarelor, dispozitivelor și sistemelor informatice deținute sau operate de Primăria Comunei Ciulnița și de instituțiile din grup.

În mod similar, această politică se aplică tuturor platformelor (sistemelor de operare) și tuturor sistemelor de aplicații.

Autentificarea

Orice utilizator (de la distanță sau intern), care trebuie să acceseze rețelele și sistemele Informatice ale instituției, trebuie să treacă prin procesul de autentificare.

Nivelul de autentificare trebuie să fie ridicat.

Autentificarea va include, dar nu se va limita la:

- Deconectarea automată;
- Un identificator unic pentru fiecare utilizator

Cel puțin una dintre următoarele:

(1) Verificare în doi factori (pași);

(2) Token;

Parolele utilizate sunt şiruri de caractere, adecvate din punct de vedere al securității ca lungime şi compoziţie, conținând majuscule și caractere speciale. Parolele nu sunt afișate pe monitor. Acestea sunt schimbate periodic, cel puțin o dată la două luni. Schimbarea periodică a parolelor se face numai de către utilizatori autorizați.

Notificare

O notificare preliminară care atrage atenția că sistemul este o rețea privată și că acei utilizatori neautorizați trebuie să se deconecteze imediat va fi afișată imediat înainte de logarea la sistem.

Aprobarea accesului

Accesul la sistem nu va fi acordat niciunui utilizator fără aprobarea corespunzătoare. Accesul utilizatorilor trebuie imediat revocat în cazul în care relația de muncă sau de colaborare cu persoana a încetat. Dacă persoana este transferată către alt sector, privilegiile trebuie modificate în mod corespunzător.

Accesul la informații

- Mijloacele de autentificare în sistem (username, parolă etc) sunt proprietatea fiecărui angajat și el este singurul responsabil de a nu divulga aceste informații.
- Este strict interzisă utilizarea credențialelor altui angajat.
- Fiecare angajat va fi responsabil să mențină securitatea oricărei informații, și în special informațiilor personale (datelor cu caracter personal) și să le protejeze de acces neautorizat (vizualizare, alterare, furt sau distrugere).
- Trebuie obținută aprobarea din partea proprietarului informației înainte de crearea, modificarea sau ștergerea unei autorizații de acces.
- Este strict interzisă copierea de fișiere electronice, iar angajatul care încalcă această regulă va fi supus sancțiunilor disciplinare, inclusiv desfacerea contractului de muncă.

- Pentru copierea fișierelor electronice, instituția își rezervă dreptul de a depune plângere penală împotriva angajatului și de a-l acționa pe acesta la instanțele civile pentru acoperirea oricărui prejudiciu adus.

- Este interzisă navigarea prin fișierele personale sau conturile altor angajați, cu excepția cazului în care acest lucru a fost aprobat în prealabil.

- Programatorii care vor dezvolta sisteme IT nu vor avea acces la date cu caracter personal, decât dacă acestea au fost anonimizate complet.

- Personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal, decât în situații excepționale și, în toate cazurile, cu respectarea tuturor obligațiilor impuse de Regulamentul (EU) 679/2016 persoanelor împuternicite și, în special, existența unor clauze contractuale exprese privind protecția datelor.

Accesul la sistem

- Notarea sau stocarea parolelor pe orice suport fizic este strict interzisă.

- Sistemul trebuie blocat ori de câte ori angajatul părăsește biroul sau nu utilizează calculatorul.

- După terminarea programului, calculatorul va fi închis. De asemenea, se va verifica faptul că închiderea s-a finalizat cu succes și fără erori.

- Este strict interzisă utilizarea „*Print screen-ului*” (prin folosirea tastei print screen sau a altor procedee) sau prin fotografierea monitorului cu telefonul pentru a salva/imprima datele cu caracter personal existente pe monitor.

- Listarea documentelor ce conțin date cu caracter personal se va realiza doar de către utilizatorii autorizați sau cu aprobarea scrisă și prealabilă a conducerii.

Consecințe

Nerespectarea prezentei Politici de către angajații companiei sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse instituției ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului. Prezenta Politică va fi adusă de către conducerea Primăriei la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 8 la Regulament

Politica privind securitatea informației

Scop

Prezentul document are scopul de a conștientiza și familiariza personalul Primăriei cu privire la metodele de protecție și securitate pentru asigurarea confidențialității, integrității și disponibilității informației. De asemenea, documentul conturează metodele acceptabile de utilizare a resurselor informatice. Resursele informaționale vor fi utilizate într-o manieră aprobată, etică și în conformitate cu prevederile legale pentru a evita pierderea sau deteriorarea operațiunilor curente, a imaginii sau a activelor financiare. Angajații trebuie să se adreseze conducerii înainte să se angajeze în orice activitate care nu este acoperită de prezenta politică.

Domeniul de aplicabilitate

Această Politică se aplică întregului personal, partenerilor de afaceri și colaboratorilor externi care au acces la sistemul informatic al instituției.

Obiective

a) Dezvoltarea unei strategii privind securitatea sistemelor informatice;

b) Promovarea standardelor etice în domeniul securității sistemelor informatice;

c) Asigurarea confidențialității, integrității și disponibilității resurselor informatice ale instituției;

d) Educarea personalului pentru a face față eficient amenințărilor cibernetice;

e) Cunoașterea riscurilor și amenințărilor venite din spațiul cibernetic;

f) Oferirea soluțiilor pentru a preveni și contracara amenințările cibernetice;

Securitatea informației

1. Accesul la echipamentele IT ale instituției de către terți se va face sub supraveghere. În contractele cu terții se vor include clauze privind măsurile de protecție a datelor și, în special, a datelor cu caracter personal;

2. Informațiile vor avea diferite grade de sensibilitate și importanță, informațiile personale (datele cu caracter personal) necesitând un nivel suplimentar de protecție;

3. Responsabilitatea angajaților privind securitatea va fi implementată încă din etapa recrutării și inclusă în contractele de muncă sau fișa postului și monitorizată permanent;

4. Parolele utilizate pentru autentificare sunt şiruri de caractere, adecvate din punct de vedere al securităţii ca lungime şi compoziţie, conținând majuscule și caractere speciale si sunt formate din cel puțin 8 caractere. Parolele nu sunt afișate pe monitor. Acestea sunt schimbate periodic, cel puțin o dată la două luni. Schimbarea periodică a parolelor se face numai de către utilizatori autorizați.

5. Angajații firmei sau alte terțe părți care au acces la sistemele informatice ale instituției trebuie să semneze un contract de confidențialitate;

6. Angajații trebuie să fie instruiți cu privire la Securitatea Informațiilor;

7. Toate incidentele de Securitate vor fi raportate conducerii, pentru a decide dacă este cazul ca acestea să fie raportate Autorității de Supraveghere și/sau persoanelor vizate. Se va implementa în acest sens o Politică privind managementul adecvat al incidentelor de Securitate;

8. Informațiile de business critice sau sensibile, precum și datele cu caracter personal trebuie să fie adăpostite în locuri sigure, protejate într-un perimetru de securitate adecvat, cu bariere de securitate corespunzătoare și controale de acces. Acestea ar trebui să fie protejate fizic împotriva accesului neautorizat, deteriorare şi interferenţe. Protecţia oferită trebuie să fie proporțională cu riscurile identificate.

9. Sistemele IT vor fi protejate împotriva amenințărilor de securitate și se vor implementa măsuri de securitate pentru a preveni și detecta accesul neautorizat in sistemele informatice si asupra datelor.

10. Trebuie să se introducă proceduri pentru efectuarea de back-up strategic, simularea periodică a restaurării de pe copiile realizate, logarea evenimentelor și a defectelor, acolo unde este posibil și monitorizarea permanentă a echipamentelor critice.

11. Utilizarea oricărui sistem IT va fi conformă legislației în vigoare cât și a normelor interne.

12. Este strict interzisă distribuirea oricăror documente interne sau alte informații către persoane neautorizate;

13. Este strict interzisă orice modificare neautorizată a echipamentelor utilizate;

14. Este strict interzisă conectarea echipamentelor personale de orice fel (hard-diskuri interne sau externe, memory stick, laptop etc) la orice echipament al organizației (PC, server, rețea internă). Nerespectarea acestei reguli aduce după sine posibilitatea desfacerii contractului de muncă sau alte măsuri disciplinare.

15. Toate sursele externe (CD, atașamente la e-mail, stick-uri, hard-disk etc) vor fi verificate cu un program anti-virus.

16. Este strict interzisă utilizarea sistemelor IT în alte scopuri decât îndeplinirea atribuțiilor de serviciu.

17. Infrastructura IT (Servere, Echipamente rețea, website) vor fi scanate de vulnerabilități si raportul de risc va fi distribuit conducerii și departamentului IT in vederea remedierii riscurilor in cel mai scurt timp. Scanările vor trebui efectuate periodic cu o recurență cel puțin semestrială.

18. Este interzisă orice intervenție asupra echipamentelor IT de către personal neautorizat de către instituție în mod scris.

19. Se interzice folosirea oricărui echipament IT de către orice persoană care nu face parte din personalul instituției fără acordul prealabil și scris al conducerii.

20. Mijloacele de autentificare în sistem (username, parolă etc) sunt proprietatea fiecărui angajat și el este singurul responsabil de a nu divulga aceste informații. De asemenea se recomandă utilizarea de sisteme de autentificare cu dublu factor (SMS,Token,etc.)

21. Este strict interzisă utilizarea credențialelor altui angajat.

22. Fiecare angajat va fi responsabil să mențină securitatea oricărei informații, și în special informațiilor personale (datelor cu caracter personal) și să le protejeze de acces neautorizat (vizualizare, alterare, furt sau distrugere).

23. Pentru copierea fișierelor electronice, instituția își rezervă dreptul de a depune plângere penală împotriva angajatului și de a-l acționa pe acesta la instanțele civile pentru acoperirea oricărui prejudiciu adus.

24. Este strict interzisă încălcarea drepturilor de autor.

25. Este interzisă navigarea prin fișierele personale sau conturile altor angajați, cu excepția cazului în care acest lucru a fost aprobat în prealabil.

26. Programatorii care vor dezvolta sisteme IT nu vor avea acces la date cu caracter personal, decât dacă acestea au fost anonimizare complet.

27. Personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal, decât în situații excepționale și, în toate cazurile, cu respectarea tuturor obligațiilor impuse de Regulamentul (EU) 679/2016 persoanelor împuternicite și, în special, existența unor clauze contractuale exprese privind protecția datelor.

28. Notarea sau stocarea parolelor pe orice suport fizic este strict interzisă.

29. Sistemul trebuie blocat ori de câte ori angajatul părăsește biroul sau nu utilizează calculatorul.

30. După terminarea programului, calculatorul va fi închis.

31. Este strict interzisă utilizarea „Print screen-ului” (prin folosirea tastei print screen sau a altor procedee) sau prin fotografierea monitorului cu telefonul pentru a salva/imprima datele cu caracter personal existente pe monitor.

32. Listarea documentelor ce conțin date cu caracter personal se va realiza doar de către utilizatorii autorizați sau cu aprobarea scrisă și prealabilă a conducerii.

33. Se va realiza back-up periodic la toate informațiile stocate pe sistemele IT.

34. Angajații nu vor uita documente pe birou care conțin date cu caracter personal după terminarea programului sau în pauză.

35. Angajații vor lua din imprimantă documentele proprii imediat după tipărire.

Consecințe

Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse instituției ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ,

sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), Societatea va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului. Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 9 la Regulament

Politica privind utilizarea internetului și a e-mail-ului

Politica

Fiecare angajat al instituției este responsabil pentru utilizarea corectă a internetului și a sistemului de poștă electronică (e-mail) și în conformitate cu această politică. Orice întrebări despre această politică ar trebui să fie adresate conducerii sau Responsabilului cu protecția datelor.

Sistemul de e-mail este proprietatea instituției. Acesta a fost furnizat Primăriei pentru utilizarea în desfășurarea activității și pentru îndeplinirea sarcinilor de serviciu. Toate comunicările și informațiile transmise de, primite de la sau stocate în acest sistem sunt înregistrări ale instituției și proprietatea acesteia. E-mailul va fi utilizat numai în scopul

îndeplinirii atribuțiilor de serviciu. Utilizarea sistemului de e-mail în scopuri personale este interzisă.
Angajații înțeleg faptul că nu au nici un drept de confidențialitate personală în orice chestiune stocată, creată, primită sau trimisă prin sistemul de e-mail al instituției.
Primăria, ca proprietar al sistemului de e-mail, își rezervă și își poate exercita dreptul de a monitoriza, accesa, prelua și șterge orice conținut stocat, creat, primit sau trimis prin sistemul de e-mail, din orice motiv și fără permisiunea unui angajat.
Chiar dacă angajații folosesc o parolă pentru a accesa sistemul de e-mail, confidențialitatea oricărui mesaj stocat, creat, primit sau trimis de la sistemul de e-mail nu poate fi asigurat. Utilizarea parolelor sau a altor măsuri de securitate nu diminuează în nici un fel drepturile instituției de a accesa materialele din sistemul său sau de a crea drepturi de confidențialitate ale angajaților în mesajele și fișierele din sistem. Orice parolă folosită de angajați trebuie să fie dezvăluită către o persoană din conducere sau unui departament organizațional, deoarece este posibil ca fișierele de e-mail să fie accesate de instituție în lipsa unui angajat.
Angajații trebuie să fie conștienți de faptul că ștergerea tuturor mesajelor sau fișierelor de e-mail nu va elimina cu adevărat mesajele din sistem. Toate mesajele de e-mail sunt stocate într-un sistem central de back-up în cursul normal al gestionării datelor.
Chiar dacă instituția are dreptul de a accesa și de a citi orice mesaje de poștă electronică, acele mesaje ar trebui să fie totuși tratate ca confidențiale de către alți angajați și accesate numai de destinatarul final. Angajații nu sunt autorizați să preia sau să citească mesajele de e-mail care nu le sunt destinate. Orice excepție de la această politică trebuie să primească aprobarea prealabilă a conducerii.
Angajații pot utiliza conexiunea la internet a companiei pentru următoarele scopuri:

- Îndeplinirea sarcinilor de serviciu;
- Utilizarea informațiilor pentru îmbunătățirea activității

Instituția nu restricționează accesul angajaților la site-urile web, dar se așteaptă ca angajații să folosească internetul în scopul îndeplinirii atribuțiilor, iar nu în scopuri personale și să rămână productivi la locul de muncă în timpul utilizării internetului.
Orice utilizare a internetului trebuie să respecte următoarele Politici:

- Politica generală privind protecția datelor cu caracter personal;
- Politica Anti-Spam;
- Politica privind accesul la date;
- Politica privind gestionarea datelor cu caracter personal;
- Politica privind securitatea informației;

Consecințe
Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici.
Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.
Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 10 la Regulament

Politica privind utilizarea dispozitivelor mobile

Introducere

Dispozitivele mobile reprezintă o componentă tot mai mare a vieții de zi cu zi, deoarece acestea devin mai puternice, iar numărul de sarcini care pot fi îndeplinite cu ajutorul lor și departe de birou crește. Cu toate acestea, pe măsură ce capabilitățile cresc, în mod evident, cresc și riscurile. Comenzile de securitate care protejează mediul desktop static nu sunt la fel de sigure atunci când se utilizează un dispozitiv mobil în afara limitelor unei clădiri de birouri.

Ca exemple de dispozitive mobile, putem enumera:

- Laptopuri.
- Notebookuri.
- Tablete.
- Smartphone-uri.
- Ceasuri inteligente.

Scopul acestei politici este de a stabili măsurile care trebuie să fie utilizate atunci când se utilizează dispozitive mobile. Se intenționează să se reducă următoarele riscuri:

- Pierderea sau furtul de dispozitive mobile, inclusiv datele pe care acestea le conțin.
- Compromiterea informațiilor clasificate prin acces neautorizat.
- Introducerea în rețea a virușilor sau a programelor malware.
- Pierderea reputației.

Este important ca măsurile stabilite în această politică să fie respectate în orice moment în utilizarea și transportul dispozitivelor mobile.

Această politică se aplică tuturor sistemelor, persoanelor și proceselor care constituie sistemele informatice ale instituției, inclusiv membrii consiliului, directorii, angajații, furnizorii și alte părți terțe care au acces la sisteme.

Dispozitive furnizate

În lipsa unei aprobări prealabile a conducerii, numai dispozitivele mobile furnizate de instituție ar trebui folosite pentru a ține sau a procesa informații clasificate în numele Primăriei.

Dacă se solicită utilizarea echipamentelor mobile se va oferi un dispozitiv corespunzător care va fi configurat să respecte politicile insitituției. Sprijinul va fi oferit de către responsabilul IT, care poate avea uneori nevoie de acces la dispozitiv pentru rezolvarea problemelor și pentru mentenanță.

Trebuie să se asigure că dispozitivul este transportat și depozitat în medii sigure și nu este expus unor situații în care acesta se poate deteriora. Nu se va lăsa aparatul nesupravegheat la vederea publicului, cum ar fi în spatele unei mașini, într-o sală de ședințe sau în hol.

Nu se va elimina niciun semn de identificare de pe dispozitiv, cum ar fi o etichetă a companiei sau o serie. Se vor lua măsuri ca dispozitivul să fie blocat și protejat de o parolă puternică.

Nu se vor stoca informații confidențiale pe dispozitiv (cum ar fi date cu caracter personal) decât dacă acest lucru a fost autorizat și dacă măsurile adecvate (de exemplu

criptarea) au fost introduse. Nu se vor păstra pe dispozitiv parolele de acces, numerele de identificare personale sau alte elemente de securitate la vedere sau ușor accesibile.
Asigurați-vă că ecranul dispozitivului se blochează după o scurtă perioadă de neutilizare și necesită un cod de acces sau o parolă pentru a-l debloca. Parolele utilizate trebuie să fie puternice și greu de ghicit. Nu se pot seta pe dispozitiv niciun fel de conectări neasigurate (adică cele care nu necesită o parolă).
Dispozitivul furnizat de instituție este destinat exclusiv destinației indicate: nu trebuie să fie împărtășită cu familia sau prietenii ori folosit pentru activități personale. Este posibil să vi se solicite să returnați dispozitivul în orice moment pentru inspecție și audit. Nu trebuie să instalați niciun software neautorizat sau să schimbați configurația sau setarea dispozitivului fără a consulta mai întâi responsabilul IT.
Acolo unde este posibil, dispozitivul va fi securizat astfel încât toate datele de pe acesta să fie criptate și să fie accesibil doar dacă parola este cunoscută. Dacă dispozitivul este livrat cu criptare, nu dezactivați criptarea.
Este posibil ca modificările aduse fișierelor deținute pe dispozitiv să nu fie însoțite în mod regulat dacă nu sunt conectate la rețeaua corporativă pentru o perioadă de timp. Încercați să programați suficient timp pentru a realiza acest lucru în mod regulat. Nu țineți propriile backup-uri necriptate de informații clasificate.
Dacă este cazul, va fi instalată pe dispozitiv o protecție împotriva virușilor. Asigurați-vă că dispozitivul este conectat periodic la rețeaua instituției pentru a permite actualizarea anti-virusului. Nu dezactivați protecția antivirus.
Dispozitivul nu trebuie să fie conectat la rețele non-corporative, cum ar fi wireless sau Internet, cu excepția cazului în care este utilizată o rețea VPN (Virtual Private Network/Rețea Virtuală Privată). Când vă aflați în locuri publice, asigurați-vă că ați amplasat dispozitivul astfel încât utilizatorii neautorizați să nu poată vizualiza ecranul sau să facă fotografii sau videoclipuri ecranului.

Utilizarea dispozitivelor mobile personale

Costul redus și disponibilitatea generală a unor astfel de dispozitive au alimentat dorința angajaților și a altor părți interesate de a-și folosi propriile dispozitive în scopuri comerciale. În unele cazuri, acest lucru poate oferi o flexibilitate sporită și poate elimina necesitatea ca angajatul să transporte mai multe dispozitive în mod regulat.
Cu toate acestea, conceptul de a permite unui angajat să utilizeze propriul dispozitiv în scopuri de afaceri poate avea ca rezultat necesitatea ca astfel de dispozitive să fie supuse unor controale suplimentare în plus față de cele care există în mod obișnuit pentru un dispozitiv de consum.
Problemele comune și problemele de securitate privind folosirea propriului dispozitiv pot include:

- utilizarea aparatului de către alți membri ai familiei
- stocarea implicită a datelor în facilitățile copiilor de rezervă în cloud
- expunerea crescută la pierderi potențiale în situații sociale, de ex. pe plajă, într-un bar
- acces potențial la site-uri care nu respectă politica de utilizare acceptabilă a instituțiilor
- conectarea la rețele nesigure, de exemplu rețele wireless nesecurizate
- inexistența unui anti-virus
- instalarea de aplicații potențial dăunătoare pe dispozitiv (de multe ori fără ca utilizatorul să fie conștient de faptul că este malware).

Aceste aspecte trebuie luate în considerare atunci când se evaluează caracterul adecvat al oricărui dispozitiv de a stoca datele confidențiale ale instituției.
Proprietarul dispozitivului și instituția vor decide dacă un anumit dispozitiv va fi utilizat în scopuri comerciale. Această utilizare nu este obligatorie, iar angajatul are dreptul de a decide dacă controalele suplimentare introduse pe dispozitiv de către instituție sunt acceptabile și, prin urmare, dacă aceștia aleg să utilizeze dispozitivul în scopuri comerciale.
Este important ca măsurile stabilite în această politică să fie respectate în orice moment în utilizarea și transportul dispozitivelor mobile. Persoanele fizice nu trebuie să utilizeze propriile dispozitive pentru a ține și prelucra informații despre instituție decât dacă au depus o cerere în acest sens și această solicitare a fost aprobată oficial. Este politica instituției să evalueze fiecare cerere în mod individual, pentru a stabili:

- identitatea persoanei care face cererea
- motivul cererii
- datele care vor fi păstrate sau procesate pe dispozitiv
- dispozitivul specific care va fi utilizat

Principiul general al acestei politici este acela că gradul de control exercitat de instituție asupra dispozitivului va fi proporțional cu gradul sensibilității datelor deținute de acesta.
Pentru a asigura că datele sale sunt protejate în mod adecvat, este important ca instituția să poată monitoriza și să verifice nivelul de conformitate cu această politică. Nivelul de monitorizare și de audit va fi adecvat clasificării informațiilor deținute pe dispozitiv.
Metodele și calendarul monitorizării vor fi stabilite astfel încât intimitatea proprietarului dispozitivului să nu fie afectată și, în toate cazurile, cu respectarea legislației în materia protecției datelor cu caracter personal. În general, monitorizarea utilizării în afara programului de lucru va fi evitată.
În cazul în care dispozitivul este pierdut sau furat, proprietarul trebuie să informeze instituția cât mai curând posibil, oferind detalii despre circumstanțele pierderii și sensibilitatea informațiilor de afaceri stocate pe acesta. Instituția își rezervă dreptul de a șterge de la distanță dispozitivul, dacă este posibil, ca măsură de precauție. Aceasta poate implica ștergerea datelor personale ale proprietarului dispozitivului.
La părăsirea Primăriei, proprietarul dispozitivului trebuie să permită ca dispozitivul să fie auditat și să fie eliminate toate datele și aplicațiile instituției.

Consecințe
Nerespectarea prezentei Politici de către angajații instituței sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici.
Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.
Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anea 11 la Regulament

Politica ANTI – SPAM

SpamMINGUL

Definiție: SPAM (în limba engleză) desemnează în general mesaje electronice trimise către o multitudine de destinatari în scopuri publicitare sau nelegale fără acordul acestora.

Ce intră în această categorie:
- mesaje publicitare nesolicitate
- mesaje ce urmăresc realizarea unei fraude prin obţinerea de date confidențiale.

Oricare dintre aceste tipuri de mesaje reprezintă o pierdere de timp, energie şi resurse pentru destinatari, furnizorii de servicii şi comunitatea utilizatorilor de Internet. Orice deținător al unui cont de email a observat că acest fenomen a scăpat de sub control.

Statisticile realizate arată că în ultimul an mesajele nesolicitate reprezintă aproximativ 70% din totalul traficului de poștă electronică.

Ce condiții trebuie să îndeplinească comunicările comerciale pentru a fi legale?

Potrivit art. 12 din Legea nr. 506/2004 și art. 6 din Legea nr. 365/2002 privind comerțul electronic, este interzisă efectuarea de comunicări comerciale prin utilizarea unor sisteme automate de apelare și comunicare, prin fax sau poștă electronică sau orice altă metodă care folosește servicii de comunicații electronice destinate publicului (mesaje SPAM), cu excepția cazului în care destinatarul și-a exprimat, în prealabil, în mod expres consimțământul pentru a primi astfel de notificări.

Consimțământul destinatarului poate fi probat cu orice mijloc de probă, însă sarcina probei revine expeditorului.

Consimțământul comunicat printr-un mesaj transmis prin poșta electronică este valabil exprimat dacă sunt îndeplinite cumulativ următoarele condiții:

a) este expediat din cutia poștala în care destinatarul dorește să primească comunicările comerciale;

b) subiectul mesajului este format din concatenarea textului "ACCEPT COMUNICĂRI COMERCIALE DIN PARTEA", scris cu majuscule, și numele sau denumirea persoanei în numele căreia se vor transmite comunicările comerciale.

Important este că destinatarul are dreptul oricând de a revoca consimțământul printr-o simplă notificare transmisă expeditorului, iar revocarea consimțământului prin mijloace electronice trebuie să-și producă efectele în cel mult 48 de ore de la inițierea procedurii.

Furnizorul are obligația de a implementa o **procedură gratuită**, accesibilă inclusiv prin mijloace electronice (*înțelegem aici inclusiv un schimb de email*), prin care destinatarul să poată să își revoce consimțământul. Furnizorul trebuie să facă publică procedura de revocare a consimțământului pe pagina proprie de Internet si în cadrul mesajelor care conțin comunicări comerciale.

Comunicările comerciale trebuie să respecte anumite condiții:

- Subiectul mesajelor transmise prin poșta electronică, care constituie comunicări comerciale, trebuie să înceapă cu cuvântul "**PUBLICITATE**" scris cu majuscule.

- Comunicările comerciale trebuie să cuprindă **cel puțin următoarele** informații referitoare la persoana în numele căreia sunt făcute:

  a) numele sau denumirea completă;

  b) codul numeric personal sau codul unic de înregistrare, după caz;

  c) domiciliul sau sediul;

  d) numerele de telefon și fax;

  e) adresa de poștă electronică.

Comunicările comerciale care constituie un serviciu al societății informaționale sau o parte a acestuia, în măsura în care sunt permise, trebuie să respecte cel puțin următoarele condiții:

- să fie clar identificabile ca atare;
- persoana fizică sau juridică în numele căreia sunt făcute să fie clar identificată;
- ofertele promoționale, precum reducerile, premiile şi cadourile, să fie clar identificabile, iar condițiile care trebuie îndeplinite pentru obținerea lor să fie ușor accesibile şi clar prezentate;
- competițiile şi jocurile promoționale să fie clar identificabile ca atare, iar condițiile de participare să fie ușor accesibile şi clar prezentate;
- orice alte condiții impuse prin dispozițiile legale în vigoare.

Măsurile luate de instituție

Instituția se angajează să nu realizeze comunicări comerciale nesolicitate.

Toate comunicările comerciale vor avea la bază consimțământul persoanei, cu excepția situației în care legea prevede altfel. Se vor implementa măsuri tehnice astfel încât consimțământul să poată fi retras la fel de simplu, precum a fost acordat. În orice caz, retragerea consimțământului își va produce efectele în cel mult 48 de ore.

Orice newsletter va avea o opțiune de dezabonare, iar orice sms va avea o modalitate de retragere a consimțământului, fie link, fie apel telefonic, fie sms.

Consecințe

Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce la sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse instituției ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 12 la Regulament

Politica de securitate fizică

Introducere

Protecția mediului fizic este una dintre cele mai importante sarcini în domeniul securității informațiilor. Lipsa controlului accesului fizic poate determina inutilitatea celor mai atente precauții tehnice și poate pune în pericol securitatea informațiilor confidențiale.
Instituția se angajează să asigure siguranța angajaților săi, a cetățenilor, a contractanților și a bunurilor și acordă o foarte mare importanță problemei securității fizice. Această politică ce stabilește principalele măsuri de precauție care trebuie luate, împreună cu documentele prezentate, formează un întreg care cuprinde setul de măsuri al securității informațiilor.
Aceste măsuri se aplică tuturor sistemelor, persoanelor și proceselor care intră în legătură cu sistemele informatice ale organizației, inclusiv membrii consiliului administrativ, directorii, angajații, furnizorii și alte părți terțe care au acces.

Zone securizate

Informațiile sensibile trebuie să fie stocate în siguranță. În ideea identificării unui nivel necesar de protecție care trebuie pus în aplicare pentru asigurarea stocării informațiilor, este imperios necesară efectuarea unei evaluări a riscurilor.

Securitatea fizică trebuie să pornească de la însăși protecția clădirii și trebuie efectuată o evaluare a vulnerabilității perimetrului. O clădire trebuie să dispună de mecanisme adecvate de control pentru păstrarea în siguranță a informațiilor confidențiale și a echipamentelor care sunt stocate în cadrul acesteia.
Acestea pot include cele de mai jos, lista nefiind exhaustivă:

- Alarme montate și activate în afara programului de lucru
- Blocări pentru ferestre și uși
- Mecanisme de control al accesului montate pe toate ușile accesibile (unde sunt utilizate codurile, acestea trebuie schimbate în mod regulat și cunoscute numai de persoanele autorizate să acceseze zona / clădirea)
- Camere CCTV
- Zonă de recepție personală
- Protecție împotriva deteriorării - de ex. incendiu, inundații, vandalism

Personalul care lucrează în zone sigure trebuie să restricționeze accesul persoanelor neautorizate.
Instrumentele de identificare și de acces (de exemplu, insigne, chei, coduri de intrare etc.) trebuie să fie deținute numai de persoane autorizate să acceseze zonele respective și nu trebuie împrumutate / furnizate nimănui altcuiva.
Vizitatorii în zonele securizate sunt obligați să declare ora de sosire și plecare și trebuie să poarte o insignă de identificare.
Cheile către toate zonele securizate care găzduiesc echipamente tehnice și departamentele tehnice sunt păstrate în condiții de maximă securitate.
În cazul în care există încălcări ale măsurilor sau un angajat și-a depășit competențele încredințate, toate instrumentele de identificare și de acces (de exemplu, insigne, chei etc.) trebuie recuperate de la angajat și toate codurile de acces trebuie schimbate imediat.

Securitatea documentelor și echipamentelor
Documentele care conțin informații confidențiale (altele decât cele electronice) trebuie protejate prin măsuri adecvate precum:

- Zone de depozitare blocate;
- Seifuri încuiate;
- Stocarea într-o zonă sigură cu acces neautorizat.

Toate echipamentele informatice trebuie amplasate în locații fizice adecvate care:

- Limitează riscurile cauzate de pericolele de mediu - de ex. căldură, foc, fum, apă, praf și vibrații;
- Limitează riscul de furt - de exemplu dacă elementele necesare, cum ar fi laptopurile, trebuie atașate fizic la birou;
- Permit posturilor de lucru care manipulează date sensibile să fie poziționate astfel încât să elimine riscul ca datele să fie văzute de persoane neautorizate.

Documentele trebuie să fie stocate și electronic. Acest lucru asigură că informațiile pierdute, furate sau deteriorate prin acces neautorizat pot fi restaurate și integritatea lor este menținută.
Toate serverele situate în afara centrului de date trebuie amplasate într-un mediu sigur din punct de vedere fizic.
Sistemele critice pentru întreprinderi trebuie să fie protejate de o sursă de alimentare continuă pentru a reduce riscul de corupție a sistemului de operare și a datelor din cauza unor defecțiuni de alimentare.
Toate echipamentele trebuie înregistrate într-un inventar. Este necesară existența unor proceduri pentru a garanta faptul că inventarul este actualizat de îndată ce activele sunt primite sau eliminate.
Toate echipamentele trebuie să fie denumite și să aibă un număr unic alocat. Acest număr de activ trebuie înregistrat în inventar.
Sistemele care transportă trebuie să fie protejate împotriva interceptării neautorizate sau deteriorării.
Cablurile de alimentare trebuie să fie separate de cablurile de rețea. Cablurile de rețea trebuie să fie protejate prin conducte și, acolo unde este posibil, să se evite rutele prin zone publice.

Gestionarea ciclului de viață al echipamentelor
Furnizorii de servicii trebuie să se asigure că toate echipamentele informatice ale instituției sunt menținute în conformitate cu instrucțiunile producătorului și cu toate procedurile interne documentate pentru a se asigura că acestea rămân în stare de funcționare eficientă.
Personalul implicat în întreținere trebuie să:

- Păstreze toate copiile instrucțiunilor producătorului
- Identifice intervalele și specificațiile recomandate
- Activeze un proces de apel în caz de eșec
- Să se asigure că numai tehnicienii autorizați finalizează orice lucrare cu privire la echipament
- Înregistreze detaliile tuturor lucrărilor de remediere efectuate
- Identifice cerințele de asigurare
- Înregistreze detaliile defecțiunilor și acțiunilor necesare

Trebuie să se păstreze o evidență a istoricului de funcționare a echipamentului, astfel încât să se poată lua decizii cu privire la momentul oportun al înlocuii acestuia.
Instrucțiunile de întreținere ale producătorului trebuie să fie documentate și disponibile pentru ca personalul de asistență să le poată utiliza la efectuarea reparațiilor.
Utilizarea echipamentelor în afara amplasamentului trebuie să fie aprobată oficial de către managerul de linie al utilizatorului.
Echipamentele care trebuie reutilizate sau eliminate trebuie să aibă toate datele șterse/ distruse. În cazul în care echipamentul urmează să fie transferat către o altă organizație (de exemplu returnat în baza unui contract de leasing), eliminarea datelor trebuie realizată utilizând instrumente software aprobate, în mod corespunzător, în siguranță.
Zona de încărcare și instalațiile de depozitare trebuie să fie protejate în mod corespunzător împotriva accesului neautorizat.
Îndepărtarea ulterioară a echipamentului trebuie să se realizeze printr-un proces formal.

Modalitățile de securitate a informațiilor trebuie să facă obiectul unor audituri regulate și independente.

Consecințe

Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 13 la Regulament

Politica privind managementul incidentelor de securitate

Introducere

Această procedură este destinată a fi utilizată atunci când a avut loc un incident de securitate care a avut ca rezultat sau există bănuieli că a dus la pierderea datelor personale pe care instituția le prelucrează.

O cerință a Regulamentului (UE) 679/2016 (GDPR) este ca incidentele de securitate cu privire la datele cu caracter personal care pot avea un risc pentru drepturile și libertățile persoanelor vizate trebuie raportate Autorității de Supraveghere (ANSPDCP) fără întârzieri nejustificate, în termen de 72 de ore de la conștientizarea acestora. În cazul în care notificarea nu poate fi făcută în 72 ore trebuie să se motiveze întârzierea. Acest document se folosește împreună cu șablonul pentru notificarea către ANSPDCP.

În cazul în care un incident afectează datele cu caracter personal, trebuie luată o decizie dacă incidentul poate conduce la un risc asupra drepturilor și libertăților persoanei fizice vizate. Regulamentul GDPR impune ca notificarea să aibă loc „fără întârzieri nejustificate" dacă încălcarea este susceptibilă să genereze „un risc ridicat pentru drepturile și libertățile persoanelor fizice". Acțiunile stabilite în acest document ar trebui utilizate numai ca îndrumare atunci când se va răspunde la un incident. Natura exactă a unui incident și impactul acestuia nu pot fi prezise cu niciun grad de certitudine și, prin urmare, este important să se utilizeze o atenție deosebită atunci când se decide ce acțiuni vor fi întreprinse. Cu toate acestea, etapele prezentate sunt utile pentru ca inituția să se asigure că obligațiile cu privire la incidentele de securitate din cadrul Regulamentului GDPR sunt îndeplinite.

Procedura de notificare a incidentelor de securitate

Odată ce s-a hotărât că a avut loc un incident de securitate asupra datelor cu caracter personal, există două aspecte cu privire la care trebuie luată decizia dacă vor fi notificate sau nu. Acestea sunt:

- Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP);
- Persoanele vizate afectate.

Nu întotdeauna un incident de securitate trebuie notificat, ci doar în situația în care incidentul prezintă un risc pentru „*drepturile și libertățile persoanelor fizice*" (articolul 33 din Regulamentul GDPR). Următoarele secțiuni descriu modul în care trebuie luată această decizie și ce trebuie făcut în cazul în care este necesară notificarea.

Decidem dacă vom notifica ANSPDCP sau nu

Regulamentul GDPR prevede că o încălcare a securității datelor cu caracter personal va fi notificată Autorității de Supraveghere „cu excepția cazului în care este puțin probabil ca încălcarea securității datelor cu caracter personal să ducă la un risc pentru drepturile și libertățile persoanelor fizice" (articolul 33 din Regulamentul GDPR). Acest lucru presupune ca instituția să evalueze nivelul riscului înainte de a decide dacă trebuie sau nu să notifice.

Factorii care trebuie luați în considerare ca parte a acestei evaluări a riscurilor ar trebui să includă:

- Datele personale au fost criptate;
- Dacă au fost criptate, cât de înalt a fost nivelul de criptare;

- În ce măsură datele au fost pseudonimizate (adică dacă persoanele pot fi, în mod rezonabil, identificate din date);

- Categoriile de date afectate (de exemplu nume, adresă, detalii bancare, date biometrice) și dacă au fost afectate categorii speciale de date;

- Volumul de date afectate;

- Numărul persoanelor vizate afectate;

- Natura incidentului (furt, pierderea unui laptop, distrugerea accidentală);

- Orice alți factori care sunt considerați relevanți.

Persoanele implicate în această evaluare a riscurilor ar trebui să includă persoane din următoarele departamente: Management, IT, Juridic, Responsabilul cu Protecția Datelor (DPO).
Metoda de evaluare a riscurilor, raționamentul și concluziile sale ar trebui să fie pe deplin documentate și semnate de conducere. Rezultatul evaluării riscurilor ar trebui să includă una dintre următoarele concluzii:

- Încălcarea datelor cu caracter personal nu necesită notificare;

- Încălcarea datelor cu caracter personal necesită doar notificarea către Autoritatea de Supraveghere (ANSPDCP);

- Încălcarea datelor cu caracter personal necesită notificarea atât Autorității de Supraveghere (ANSPDCP), cât și persoanelor vizate.

Aceste concluzii pot fi supuse schimbării bazate pe feedbackul Autorității de Supraveghere (ANSPDCP) sau ulterior, ca urmare a descoperirii altor informații suplimentare din care rezultă că impactul este grav și incidentul prezintă un risc asupra persoanelor fizice.

Cum notificăm Autoritatea de Supraveghere

În cazul în care se decide să se realizeze notificarea către Autoritatea de Supraveghere, o cerință a Regulamentului GDPR este că incidentele de securitate cu privire la datele cu caracter personal care pot avea un risc pentru drepturile și libertățile persoanelor vizate trebuie raportate Autorității de Supraveghere (ANSPDCP) fără întârzieri nejustificate, în termen de **72 de ore de la conștientizarea acestora**. În cazul în care notificarea nu poate fi făcută în 72 ore trebuie să se motiveze întârzierea.
Notificarea se va realiza la adresa de e-mail brese@dataprotection.ro, cu excepția cazului în care ANSPDCP va indica o altă modalitate pentru transmiterea notificării.
Notificarea va cuprinde, cel puțin, următoarele:

(a) caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

(b) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

(c) consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Se va utiliza formularul de notificare furnizat sau, în situația în care ANSPDCP va furniza un model de formular, acesta din urmă. De asemenea, există un formular de notificare online, disponibil la adresa:
http://www.dataprotection.ro/servlet/ViewDocument?id=1100.

Decidem dacă vom notifica persoanele vizate sau nu

Regulamentul GDPR afirmă „în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un ***risc ridicat*** pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare." Prin urmare, notificarea ANSPDCP se va face atunci când incidentul de securitate prezintă un risc, iar notificarea persoanelor vizate se va realiza atunci când incidentul prezintă un ***risc ridicat.***

Factorii care trebuie luați în considerare ca parte a acestei evaluări a riscurilor ar trebui să includă:

- Datele personale au fost criptate;
- Dacă au fost criptate, cât de înalt a fost nivelul de criptare;
- În ce măsură datele au fost pseudonimizate (adică dacă persoanele pot fi, în mod rezonabil, identificate din date);
- Categoriile de date afectate (de exemplu nume, adresă, detalii bancare, date biometrice) și dacă au fost afectate categorii speciale de date;
- Volumul de date afectate;
- Numărul persoanelor vizate afectate;
- Natura incidentului (furt, pierderea unui laptop, distrugerea accidentală);
- Orice alți factori care sunt considerați relevanți.

Persoanele implicate în această evaluare a riscurilor ar trebui să includă persoane din următoarele departamente: Management, IT, Juridic, Responsabilul cu Protecția Datelor (DPO). Aceste concluzii pot fi supuse schimbării bazate pe feedbackul Autorității de Supraveghere (ANSPDCP) sau ulterior, ca urmare a descoperirii altor informații suplimentare din care rezultă că impactul este grav și incidentul prezintă un risc ridicat asupra persoanelor fizice.

Notificarea persoanelor vizate nu este obligatorie în situația în care ar necesita „eforturi disproporționate" din partea operatorului.

Cum notificăm persoanele vizate

Odată ce s-a decis că trebuie notificate persoanele vizate Regulamentul GDPR cere ca acest lucru să se facă fără întârzieri nejustificate. Comunicarea către persoanele vizate afectate va descrie în limbaj simplu și clar natura încălcării securității datelor cu caracter personal (articolul 34 din Regulamentul GDPR) și trebuie să cuprindă și:

(a) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

(b) consecințele probabile ale încălcării securității datelor cu caracter personal;

(c) măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

În plus față de punctele solicitate de Regulamentul GDPR, ar putea fi oportun să se ofere ajutor persoanei vizate cu privire la acțiunile pe care acestea le pot lua pentru a reduce riscurile asociate cu încălcarea securității datelor cu caracter personal.
În majoritatea cazurilor, este oportună notificarea persoanelor vizate afectate prin poștă, e-mail sau ambele, pentru a se asigura că mesajul a fost primit și că au posibilitatea de a lua orice acțiune necesară.

Consecințe
Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici.
Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.
Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela

Anexa 14 la Regulament

Procedura privind supravegherea prin mijloace video

Introducere
Această politică stabileşte:

- un set unitar de reguli care reglementează implementarea şi utilizarea sistemului de supraveghere video în scopul asigurării securităţii persoanelor şi bunurilor, pazei şi protecţiei bunurilor, imobilelor, valorilor şi a materialelor cu regim special care sunt utilizate în activitate, respectând în același timp obligațiile ce revin Primăriei Comunei Ciulnița în calitate de operator de date, conform legislației din domeniul protectiei datelor şi măsurile de securitate adoptate pentru protecţia datelor cu caracter personal, protejarea vieţii private, a intereselor legitime şi garantarea drepturilor fundamentale ale persoanelor vizate

- responsabilităţile privind administrarea şi exploatarea sistemului de supraveghere prin mijloace video, precum şi cele privind întocmirea, avizarea şi aprobarea documentelor aferente acestor activităţi

Politica privind supravegherea prin mijloace video descrie sistemul video al Primăriei Comunei Ciulnița şi măsurile de protecţie luate de instituție pentru a proteja datele cu caracter personal, viaţa privată şi alte drepturi fundamentale şi interese legitime ale persoanelor filmate de camerele de supraveghere.

Domeniul

Politica se aplică în cadrul activităţii de supraveghere prin mijloace video, corespunzător competenţelor, de către:

- ❖ personalul desemnat cu administrarea sistemului
- ❖ conducerea unității
- ❖ personalul intern care asigură paza perimetrelor
- ❖ personalul intern care asigură mentenanţa sistemelor de supraveghere

Supravegherea prin mijloace video se utilizează doar în situaţia în care mijloacele convenţionale aplicate sunt considerabil mai puţin eficiente în realizarea obiectivelor menţionate, conform analizei de risc efectuate la nivelul instituţiei.

Primăria Comunei Ciulnița prelucrează imaginile înregistrate respectând prevederile legale în domeniu.

Referințe normative

a) Legea nr. 333 din 8 iulie 2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, cu modificările şi completările ulterioare;

b) Hotărârea nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor Metodologice a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor

c) Instrucţiunile Autorităţii Europene de Protecţie a Datelor Personale privind supravegherea video, publicate 17 martie 2010, Bruxelles;

d) Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date;

e) Legea nr. 190/2018 privind măsuri de punere în aplicare la nivel național a Regulamentului (UE) 679/2016;

f) Legea nr. 135/2010 privind Codul de procedură penală;

g) Legea nr. 286/2009 privind Codul penal;

h) Legea nr. 155/2010 privind legea poliției locale;

i) Hotărârea 1332/2010 privind aprobarea Regulamentului de organizare și funcționare a poliției locale.

Utilizarea sistemului video este necesară pentru buna administrare şi funcţionare a Primăriei Comunei Ciulnița, în special în vederea controlului de securitate şi pază descris în secţiunile de mai jos.

Transparența

Politica privind utilizarea sistemelor video este disponibilă pe pagina de internet a instituției.

Zonele supravegheate

Sistemul de supraveghere prin mijloace video cuprinde urmatoarele locatii:

- ➢ *În incinta şi împrejurimile sediului Primăriei Comunei Ciulnița, județul Ialomița.*
- ➢ *În puncte fixe din interiorul Comunei Ciulnița.*

Condiții de legitimitate

Se supraveghează prin mijloace video:

- ❖ zonele de acces
- ❖ casieriile si seifurile metalice din dotarea lor
- ❖ împrejurimile clădirilor, pentru a proteja spaţiile exterioare

- perimetrul interior al birourilor,
- camera serverelor

Amplasarea camerelor a fost atent revizuită pentru a asigura limitarea pe cât posibil a monitorizării zonelor care nu prezintă interes pentru scopul urmărit

Dispozitivul de înregistrare este amplasat într-un spaţiu aflat sub pază permanentă, a societății contractante privind furnizarea acestor servicii. Nu sunt monitorizate zonele în care există un nivel ridicat al aşteptărilor privind viaţa privată, precum birourile, toaletele şi alte locaţii similare.

Datele cu caracter personal colectate prin intermediul supravegherii video

1.1..a.i.1. **Scopul supravegherii prin mijloace video**

Primăria Comunei Ciulnița utilizează sistemul de supraveghere video doar în scop de securitate şi control acces.

Cu ajutorul acestui sistem se controlează accesul în incinta unităţii, se asigură securitatea bunurilor şi siguranţa persoanelor – angajaţi, cetățeni, vizitatori, prestatori de servicii din cadrul altor firme. În plus, sistemul de supraveghere video ajută la prevenirea, detectarea şi investigarea furturilor de echipamente sau bunuri deţinute de instituţie sau la prevenirea, detectarea şi investigarea riscurilor şi ameninţărilor la adresa personalului angajat care îşi desfăşoară activitatea la locaţia supravegheată.

2. **Limitarea scopului**

Sistemul de supraveghere video nu este utilizat în alt scop decât cel notificat, nu foloseşte la monitorizarea activităţii angajaţilor sau la pontaj. Mai mult, sistemul poate constitui mijloc de investigare sau de obţinere a unor informaţii pentru anchetele interne sau procedurile disciplinare, inclusiv in cazul situaţiilor în care se produce un incident de securitate fizică sau se observă un comportament infracţional (în circumstanţe excepţionale imaginile pot fi transferate organelor de cercetare în cadrul unei investigaţii disciplinare sau penale).

3. **Categorii speciale de date**

Sistemul video al Primăriei Comunei Ciulnița nu are ca scop captarea (de exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (de exemplu, indexare, creare de profiluri) care dezvăluie „categorii speciale de date".

4. **Descrierea şi specificaţiile tehnice ale sistemului**

În mod convenţional sistemul de supraveghere video este un sistem static. Are ca funcţie înregistrarea imaginilor şi este echipat cu senzori de mişcare. Sistemul poate înregistra orice mişcare detectată de camerele instalate în zona supravegheată, alături de dată, oră şi locaţie.Toate camerele sunt funcţionale 24 de ore, 7 zile pe săptămână.

Atunci când este necesar, calitatea imaginilor permite recunoaşterea celor care trec prin zona de acţiune a camerelor. Pentru o mai mare siguranţă a prelucrării datelor care pot fi obţinute în urma supravegherii video, camerele sunt fixe (fără funcţie de zoom), astfel utilizatorul nu poate modifica perimetrul/ scopul supravegherii. Sistemul este utilizat de către paznici doar pentru supraveghere, ei nu au dreptul de operare a sistemului sau de a consulta inregistrările sistemului.

5. **Beneficiile sistemului de supraveghere:**

- Creşterea controlului în perimetrul supravegheat, a intrărilor şi ieşirilor
- Eliminarea pierderilor cauzate de evenimente neprevăzute
- Respectarea actelor, normativelor şi legislaţiei în vigoare pentru obiectivele cu risc.

Instalarea, administrarea, exploatarea sistemului

În vederea asigurării unei protecţii eficiente a drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în cadrul operaţiunilor de supraveghere video a căilor publice de acces şi a spaţiilor publice deschise este interzisă prelucrarea de imagini care să vizualizeze interiorul imobilelor locuite sau a căilor de acces în acestea.
Echipamentele sunt astfel instalate încât să se afle sub supraveghere doar acele spaţii identificate în analiza de risc ca având nevoie de protecţie suplimentară.
Imaginile captate de sistemul de supraveghere video sunt vizualizate și colectate doar în sistemul de la punctul de control, iar monitoarele nu pot fi văzute din exterior.
Nu este permis accesul neautorizat la sistemul video.
Accesul este strict limitat la angajaţii autorizaţi, administratorii de sistem şi conducerea instituției, precum și reprezentanții firmei care asigură mentenanța sistemului, însoțiți de unul din administratorii sistemului.
De la caz la caz, se poate acorda accesul la sistemul video şi altor persoane, în afara celor menţionate mai sus, doar pe bază de autorizare din partea conducerii unității, dupa ce s-a obtinut aprobarea Responsabilul cu Protecţia Datelor cu Caracter Personal . Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video.

Protejarea vieţii private şi securitatea informaţiilor

Pentru a proteja securitatea sistemului video şi pentru a spori gradul de protecţie a vieţii, au fost introduse următoarele **măsuri tehnice şi organizatorice**:

- **limitarea timpului de stocare a materialului filmat la o durata de 30 de zile**
- toţi utilizatorii cu drept de acces au semnat **declaraţii de confidenţialitate** , prin care se obligă să respecte prevederile legale în domeniu
- dreptul de acces se acordă utilizatorilor pe baza nevoii de a cunoaşte, doar pentru acele resurse care sunt strict necesare pentru îndeplinirea atribuţiilor de serviciu
- doar administratorul de sistem, numit în acest sens de către operator, are dreptul de a acorda, modifica sau anula dreptul de acces al utilizatorilor, conform procedurii generale de acces la bazele de date. Acesta tine în permanență o listă actualizată a tuturor persoanelor care au drept de acces la sistemul de supraveghere video, cu specificarea tipului de acces.

Responsabilul cu Protecţia Datelor cu Caracter Personal va fi consultat înainte de achiziţionarea sau instalarea oricărui nou sistem video de protecţie.

Accesul la datele personale şi dezvăluirea acestora

1. Drepturi de acces

Accesul la imaginile stocate şi/sau la arhitectura tehnică a sistemului de supraveghere video este limitat la un număr redus de persoane şi este determinat prin atribuţiile specificate în fişa postului (în ce scop şi ce tip de acces). În special, Primăria Comunei Ciulnița impune limite în privinţa persoanelor care au dreptul:

- să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile paznicilor desemnaţi să desfăşoare 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 şi incidentele de securitate, de către persoanele special desemnate
- să copieze, să descarce, să şteargă sau să modifice orice material filmat

2. Măsuri de păstrare a confidenţialităţii

Administratorii sistemului semnează o declaraţie de confidenţialitate.

3. 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 (de securitate şi control acces), dar numai după ce a fost consultat Responsabilul cu Protecţia Datelor cu Caracter Personal.
Primăria Comunei Ciulnița are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, a înregistrărilor video în care este surprinsă săvârşirea unor fapte de natură penală, dar numai dupa consultarea Responsabilului cu Protecţia Datelor cu Caracter Personal.
Sistemul de supraveghere 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 Comisiei Disciplinare, în cadrul unei anchete disciplinare, cu condiţia ca informaţiile să ajute la investigarea unei infracţiuni sau a unei abateri disciplinare de natură să prejudicieze drepturile şi libertăţile unei persoane.
Orice încălcare a securităţii în ceea ce priveşte camerele video este indicată în Registrul de evenimente al sistemului.

Durata de stocare

Durata de stocare a datelor obţinute prin intermediul sistemului de supraveghere video este proporţională cu scopul pentru care se prelucrează datele, astfel că imaginile sunt stocate pentru o perioadă care nu depăşeşte 30 de zile, după care se şterg prin procedură automată în ordinea în care au fost înregistrate. În cazul producerii unui incident de securitate, durata de păstrare a materialului filmat relevant poate depăşi limitele normale în funcţie de timpul necesar investigării suplimentare a incidentului de securitate. Păstrarea este documentată riguros, iar necesitatea păstrării este revizuită periodic.

Drepturile persoanei vizate

Primăria Comunei Ciulnița garantează și asigură respectarea drepturilor ce revin personelor vizate, conform legii. Toate persoanele implicate în activitatea de supraveghere video şi cele responsabile de administrarea imaginilor filmate, vor respecta Procedura de acces la datele cu caracter personal.

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 încât să semnaleze existenţa camerelor de supraveghere, dar şi pentru a comunica informaţiile esenţiale privind prelucrarea datelor personale. Persoanele vizate sunt atenţionate asupra existenţei sistemului de supraveghere video şi prin note de informare corespunzătoare, care cuprind scopul prelucrării şi identifică instituția ca operator al datelor colectate prin intermediul supravegherii video.

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 instituție, 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 Responsabilului cu Protecţia Datelor cu Caracter Personal și instituției.
Răspunsul la solicitarea de acces, intervenţie sau opoziţie se dă în termen de 30 zile calendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amânare 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 prejudicia drepturile terţilor (persoana vizată va putea vizualiza doar propria imagine, imaginile

altor persoanelor care pot apărea în înregistrare vor fi editate astfel încât 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 când 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 încât 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 încât 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 consimţământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante. Prezenta politică de supraveghere prin mijloace video va fi adusă la cunoștință tuturor angajaților Primăriei Comunei Ciulnița și a altor persoane vizate. De asemenea, va fi afișată și pe site-ul instituției, spre informarea tuturor persoanelor interesate.

PREŞEDINTE DE ŞEDINŢĂ,
Fieraru Ion-Albert

Contrasemnează,
Pt.Secretar general al comunei,
Chițu Nela