

ROMÂNIA



JUDEȚUL ARAD

**CONSILIUL LOCAL AL COMUNEI IGNEȘTI**

ROMÂNIA Județul Arad comuna Ignești nr. 24 cod poștal 317195 tel/fax 0257 315521

E-mail: primaria.ignesti@yahoo.com Site: www.primariaignesti.ro

**HOTĂRÂREA nr.39****Din 28.06.2021****cu privire la aprobarea Regulamentului general privind protecția datelor cu caracter personal.**

Consiliul local al comunei Ignești, Jud.Arad

Avand in vedere :

-Raportul de specialitate pentru aprobarea Regulamentului privind protecția datelor cu caracter personal precum și proiectul Regulamentului privind protecția datelor cu caracter personal întocmit de responsabilul cu protecția datelor cu caracter personal;

- prevederile Regulamentului (UE) 2016/679 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) 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);

- art.25 din Ordinul nr.25/2021 a Ministerului Dezvoltării, Lucrarilor Publice si Administratiei

-prevederile art.129 alin ,14 din O.U.G.nr.57/2019 privind Codul administrativ;

- votul **favorabil** exprimat de un numar de 9 consilieri locali, din cei 9 consilieri prezenti la lucrarile sedintei;

In temeiul art. 139 din O.U.G.nr.57/2019 privind Codul administrativ;

**HOTĂRĂȘTE :**

**Art.1.** Consiliul Local al comunei Ignești aprobă Regulamentul privind protecția datelor cu caracter personal, conform anexei nr.1, anexă care face parte integrantă din prezentul proiect.

**Art.2.** Prezenta se comunica :

-Institutiei Prefectului Judetului Arad

-Primarului Comunei Ignești

-prin afisare publica

**PREȘEDINTE DE ȘEDINȚĂ,**

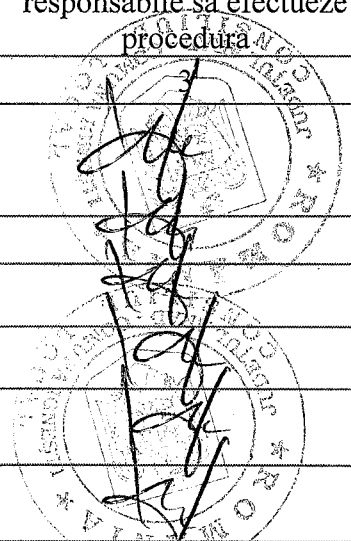
Consilier,

Urs Daniel-Cristian



**ANEXA Nr. 9  
la regulament**

**Cartuș cu proceduri obligatorii ulterioare adoptării hotărârii consiliului local**

PROCEDURI OBLIGATORII ULTERIOARE ADOPTĂRII HOTĂRÂRII CONSILIULUI LOCAL NR.39 /2021 <sup>1</sup>			
Nr. crt.	Operațiuni efectuate	Data ZZ/LL/AN	Semnătura persoanei responsabile să efectueze procedura
0	1	2	
1	Adoptarea hotărârii <sup>1)</sup> s-a făcut cu majoritate <input type="checkbox"/> simplă <input type="checkbox"/> absolută <input type="checkbox"/> calificată <sup>2)</sup>	28 /06/2021	
2	Comunicarea către primar <sup>2)</sup>	28/06/2021	
3	Comunicarea către prefectul județului <sup>3)</sup>	09/07/2021	
4	Aducerea la cunoștința publică <sup>4)+5)</sup>	28/06/2021	
5	Comunicarea, numai în cazul celei cu caracter individual <sup>4)+5)</sup>	28/06/2021	
6	Hotărârea devine obligatorie <sup>6)</sup> sau produce efecte juridice <sup>7)</sup> , după caz	28/06/2021	

## REGULAMENT GENERAL PRIVIND PROTECTIA DATELOR CU CARACTER PERSONAL

### 1. Introducere

Primăria Comunei Ignești prelucrează date cu caracter personal referitoare atât la persoane fizice, cât și la persoane juridice. Acestea pot reprezenta date în legătură cu contribuabilii, furnizorii, beneficiarii de servicii publice, angajați și alte persoane sau instituții cu care Primăria a încheiat un contract sau cu care aceasta se află într-o legătură.

Acest Regulament descrie modul în care datele personale trebuie colectate, utilizate și stocate pentru a fi în concordanță cu standardele companiei 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 Comunei Ignești.

Următoarele proceduri sunt relevante pentru a implementa Regulamentul General privind Protecția Datelor cu Caracter Personal :

- *Procedura privind protecția datelor cu caracter personal*
- *Procedura privind conformitatea cu cerințele legale*
- *Procedura privind securitatea IT*
- *Procedura de Back-up*
- *Procedura privind evaluarea impactului*
- *Procedura de cartografiere a datelor cu caracter personal*
- *Procedura de gestionare a cererilor persoanelor vizate*
- *Procedura de notificare a confidențialității datelor cu caracter personal*
- *Procedura de asigurare a securității datelor cu caracter personal*
- *Procedura privind gestionarea și stacarea datelor cu caracter personal*
- *Procedura de răspuns la incidentele de securitate*
- *Procedura privind gestionarea și raportarea incidentelor de securitate*
- *Procedura privind prelucrarea datelor cu caracter personal colectate prin sistemul de supraveghere video*
- *Procedura privind evaluarea și contractarea persoanelor împuternicite*
- *Procedura privind aplicarea GDPR în cadrul instituției*
- *Procedura de sistem privind Elaborarea procedurilor, circuitul și controlul documentelor – ediția în vigoare*
- *Procedura de sistem privind controlul înregistrărilor – ediția în vigoare*

- *Roluri și responsabilități în GDPR*

## 2. Existența Regulamentului

Acest Regulament privitoare la protecția datelor asigură Primăria Comunei Ignești de:

- Conformitatea cu legislația privind protecția datelor cu caracter personal și practicile performante la acest nivel;
- Protecția drepturilor persoanelor vizate: de exemplu a partenerilor, contribuabililor, angajaților;
- Modul de stocare și prelucrare a datelor persoanelor fizice;
- Protecția primăriei de posibilele riscuri referitoare la încălcarea securității datelor.

## 3. Legislația privitoare la protecția datelor cu caracter personal

**Regulamentul (EU) nr. 679/2016** descrie modul în care organizațiile – incluzând Primăria Comunei Ignești 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.

#### 4. Definiții

Există un număr total de 26 de definiții enumerate în cadrul GDPR și nu este adecvată reproducerea acestora aici. Cu toate acestea, definițiile cele mai fundamentale cu privire la acest regulament sunt următoarele:

<b>Date cu caracter personal</b>	orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”)
<b>Persoana vizată</b>	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
<b>Prelucrare</b>	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
<b>Operator</b>	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
<b>Persoană împuternicită de operator</b>	persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului

## 5. 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:

- prelucrate în mod legal, echitabil și transparent față de persoana vizată („**legalitate, echitate și transparență**”);
- 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**”);
- adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („**reducerea la minimum a datelor**”);
- 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**”);
- 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**”);
- 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 Ignești 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.

## 6. 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 cadrul Primăriei Comunei Ignești 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 servicii poștale, adresate Primăriei, ca operator de date, la adresa declarata. Primăria poate atașa o cerere standard, cu toate că persoanele nu sunt obligate să o folosească.

Cererile vor fi scutite de vreo taxă. Primăria va fi obligată să furnizeze răspuns în maxim 30 de zile, iar în anumite cazuri excepționale în cel mult două luni de la primirea cererii.

Primăria va verifica întotdeauna identitatea oricărei persoane. În vederea răspunderii la cereri și permiterea exercitării drepturilor, Secretarul General al U.A.T. sau consultanții juridici vor avea un cuvânt de spus cu privire la temeinicia cererii.

Primăria Comunei Ignești respectă următoarele termene pentru răspunsul la cererile persoanelor vizate:

Solicitarea de date solicitate	Grafic de timp
<i>Dreptul de a fi informat</i>	Atunci când se colectează date (dacă acestea sunt furnizate de persoana vizată) sau în termen de 30 de zile (dacă nu sunt furnizate de persoana vizată)
<i>Dreptul de acces</i>	30 de zile
<i>Dreptul la rectificare</i>	30 de zile
<i>Dreptul de ștergere</i>	Fără întârzieri nejustificate
<i>Dreptul de a restricționa procesarea</i>	Fără întârzieri nejustificate
<i>Dreptul la portabilitatea datelor</i>	30 de zile
<i>Dreptul de a se opune prelucrării</i>	La primirea obiecției
<i>Drepturi legate de procesul de luare a deciziilor și profilaxie automată.</i>	Nespecificat

**7. 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
- Activitatea desfășurată în interes public
- Obligația legală
- Interesul legitim
- Interesele vitale ale subiectului
- Încheierea sau executarea unui contract

#### • **Consimțământul**

Cu excepția cazului în care este necesar dintr-un motiv admis în Regulamentul GDPR, Primăria Comunei Ignești 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 noastre 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.

#### • **Activitatea desfășurată în interes public**

În cazul în care Primăria Comunei Ignești 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.

#### • **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 cazul în cazul anumitor date referitoare la ocuparea forței de muncă și la impozitare, de exemplu.

#### • **Interesul legitim**

Dacă prelucrarea datelor cu caracter personal specific este în interesul legitim al Primăriei Comunei Ignești 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.

- **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 temeiul legal al prelucrării. Primăria Comunei Ignești va păstra dovezi rezonabile, documentate că acest lucru este cazul, ori de câte ori acest motiv este utilizat ca bază legală pentru prelucrarea datelor cu caracter personal.

- **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, *de exemplu* o livrare nu poate fi efectuată fără o adresă la care să se poată livra.

## 8. **Persoane fizice, riscuri și responsabilități**

- o **Domeniul Regulamentului**

Prezentul Regulament se aplică:

- Sediului Primăriei Comunei Ignești
- Tuturor compartimentelor Primăriei Comunei Ignești
- Întregului personal și voluntarilor Primăriei Comunei Ignești
- Tuturor contractanților, furnizorilor și altor autorități ce lucrează în numele Primăriei Comunei Ignești

Are aplicabilitate asupra tuturor datelor pe care Primăria 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**

Regulamentul ajută la protejarea Primăriei Comunei Ignești de reale riscuri la nivel de securitate, incluzând:

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

- **Responsabilități**

Oricine lucrează pentru sau cu Primăria Comunei Ignești își angajează răspunderea pentru a asigura colectarea, stocarea și utilizate 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:

- *Primăria* este responsabilă cu privire la asigurarea îndeplinirii în mod legal a obligațiilor de către Primăria Comunei Ignești

- *Responsabilul cu protecția datelor cu caracter personal* numit prin dispoziție este responsabil cu
- Informarea, sfătuiră 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 organizației;
- 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 compartimente 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 organizației 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 menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune;
- Asumarea rolului de punct de contact cu persoanele vizate privind la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor 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.

- *Primarul*, este responsabil 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 continuă 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 compania îl 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;
- Trimiterea de răspunsuri asupra oricăror interogări ce provin de la jurnaliști sau puncte de vânzare media precum ziare;
- Unde este necesar, lucrul cu alt personal pentru a asigura respectarea principiilor privitoare la protecția datelor cu caracter personal în legătura cu inițiativele de marketing.

#### • **Regulamentul general al personalului**

- Singurele persoane care sunt apte să acceseze datele prezentate în acest Regulament ar trebui să fie cele cărora le este necesară pentru activitatea pe care o realizează.

- Datele ar trebui să nu fie împărtășite către toți angajații. Când este necesar accesul la informații confidențiale, angajații pot solicita direct de la managerii lor.
- Primăria Comunei Ignești 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 ar trebui 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 companiei sau în afară.
- Datele ar trebui 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 lor sau responsabilului cu protecția datelor dacă nu sunt siguri în legătura cu orice aspect al protecției datelor.

## 9. 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 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 ar trebui păstrate într-un loc închis sau într-un sertar închis;
- Angajații ar trebui să se asigure că hârtia sau cele printate nu sunt lăsate către oameni neautorizați ce ar putea să le vadă, ca de exemplu pe imprimantă;
- Printurile ar trebui distruse când nu mai sunt necesare.

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

- Datele ar trebui protejate de parole puternice ce sunt schimbate regulat și niciodată împărtășite între angajați;
- Dacă datele sunt stocate pe suporturi amovibile (precum CD, DVD), acestea ar trebui păstrate în siguranță atunci când nu sunt folosite;
- Datele ar trebui stocate numai în servere sau unități specializate și ar trebui să fie încărcate într-un serviciu de cloud computing aprobat;
- Serverele ce conțin informații personale ar trebui plasate într-un loc sigur, departe de spațiul general de birouri;
- Datele nu ar trebui salvate direct pe laptopuri sau alte dispozitive mobile precum tablete sau telefoane inteligente.
- Datele ar trebui să aibă copie de siguranță. Aceste copii de siguranță trebuie testate regulat.

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

## 10. Utilizarea datelor

Datele personale nu au nicio valoare pentru Primărie 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 ar trebui să asigure ecranele calculatoarelor întotdeauna închise când le lasă nesupravegheate;
- Datele personale nu ar trebui transmise prin e-mail, având în vedere că aceasta cale de comunicare nu este sigură.
- Datele ar trebui criptate înainte de a fi transferate electronic. Responsabilul IT ar trebui să explice cum sunt trimise datele către contactele externe autorizate.
- Datele personale nu ar trebui transferate în afara Spațiului Economic European.
- Angajații ar trebui să nu salveze datele personale în dispozitivele lor personale. Întotdeauna ar trebui să existe acces și actualizare a copiei centrale a tuturor datelor.

## 11. Precizia datelor

Legislația solicită Primăriei Comunei Ignești 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 Primăriei Comunei Ignești 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 ar trebui să se folosească de fiecare oportunitate pentru a asigura actualizarea datelor. *De exemplu*, prin confirmarea unor detalii în momentul în care clientul sună;
- Primăria Comunei Ignești va depune toate diligențele necesare pentru ca subiectele datelor să își poată actualiza informațiile pe care Primăria Comunei Ignești le deține. *De exemplu*, prin intermediul site-ului web al instituției;
- Datele ar trebui actualizate când se descoperă inadvertențe. De exemplu, când un client nu mai poate fi contactat prin intermediul unui număr de telefon, se recomandă eliminarea din baza de date a acestuia.

## 12. 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 Ignești va dezvălui datele necesare. Operatorul de date va asigura faptul că cererea este legitimă, căutând asistență unde este necesar.

### 13. Furnizare informații

Primăria Comunei Ignești 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, compania are o *procedură privind confidențialitatea*, stabilind cum datele indivizilor sunt utilizate în cadrul acesteia.

### 14. Consecințe

Nerespectarea prezentului Regulament de către angajații Primăriei 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 prezentului Regulament cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), Primăria Comunei Ignești va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

Prezentul Regulament va fi adus de către responsabilul cu protecția datelor la cunoștința tuturor angajaților, colaboratorilor sau a altor terți.

Întocmit,

Responsabil Protecția DCP,

C.J.FEIER ADELA

