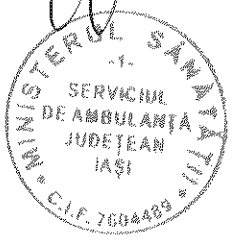
Serviciul de Ambulanță Județean Iași	Aprob Manager General, Dr.Hristea Angelica	Ediția I Revizia 0



PROCEDURĂ OPERAȚIONLĂ

Prelucrarea Datelor cu Caracter Personal în cadrul Serviciului de Ambulanță Județean Iași

GDPR

COD: P0 S.A.J. 02

Ediția 1

Revizia 0

Elaborat:
Responsabil GDPR,
Ec.Elihayrat Petronela

PROCEDURĂ OPERAȚIONLĂ

Prelucrarea Datelor cu Caracter Personal în cadrul Serviciului de Ambulanță Județean Iași

GDPR

I. Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii documentate

Nr. Crt	Elemente privind responsabilii/ operațiunea	Numele și prenumele	Funcția	Data	Semnătura
1	2	3	4	5	6
1.1	Elaborat	Elihayrat Petronela	Economist Responsabil GDPR(DPO)	15.05.2024	
1.2	Verificat	Crihan Marlena	Director Medical	15.05.2024	
1.3	Aprobat	Hristea Angelica	Manager General	15.05.2024	

II. Situația edițiilor și a reviziilor în cadrul edițiilor procedurii

Nr. Crt	Ediția sau, după caz, revizia în cadrul ediției	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediției sau reviziei ediției
1	2	3	4	5
2.1	Ediția I-a			
2.2	Revizia 0			
2.3	Revizia 1			

III. Lista de distribuire a procedurii

Nr. crt.	Compartimentul[1]	Numele și prenumele personalului de conducere	Data distribuirii	Modul distribuirii (prin e-mail, în format hârtie, postare intranet etc.)
1	Tuturor compartimentelor			1) prin e-mail

IV. Scopul și obiectivul procedurii

1. Scopul procedurii

Scopul prezentei proceduri este de a reglementa, într-un mod unitar și conform prevederilor legale în vigoare, activitățile de prelucrare a datelor cu caracter personal desfășurate în cadrul Serviciului de Ambulanță Județean Iași, în vederea implementării prevederilor Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

Această procedură are următoarele obiective principale:

- Stabilirea cadrului normativ intern pentru desfășurarea legală, echitabilă și transparentă a prelucrărilor de date cu caracter personal;
- Asigurarea respectării principiilor fundamentale prevăzute de GDPR, inclusiv limitarea scopului, minimizarea datelor, exactitatea, limitarea stocării, integritatea și confidențialitatea;
- Definirea clară a responsabilităților angajaților care prelucrează date cu caracter personal în exercitarea atribuțiilor lor profesionale;
- Garantarea exercitării drepturilor persoanelor vizate și stabilirea mecanismelor interne pentru soluționarea cererilor acestora;
- Crearea unui cadru coerent pentru identificarea, evaluarea și reducerea riscurilor asociate prelucrării datelor;
- **Stabilirea modalităților de întocmire, completare, actualizare și păstrare a Registrului de evidență a activităților de prelucrare a datelor cu caracter personal,** defalcat pe compartimente funcționale din cadrul instituției, astfel încât să se asigure trasabilitatea și transparența proceselor de prelucrare;
- Asigurarea unui instrument intern de auditare și control al conformității, prin menținerea unui registru complet și actualizat, conform art. 30 din Regulamentul (UE) 2016/679.

PROCEDURĂ OPERAȚIONLĂ

Prelucrarea Datelor cu Caracter Personal în cadrul Serviciului de Ambulanță Județean Iași

GDPR

Această procedură contribuie la consolidarea unei culturi instituționale bazate pe responsabilitate, conformitate cu reglementările europene și naționale, precum și pe respectarea drepturilor fundamentale ale persoanei, în special dreptul la viață privată și protecția datelor cu caracter personal.

Obiectiv

Procedura asigură:

1. Identificarea tuturor activităților de prelucrare a datelor cu caracter personal în cadrul compartimentelor și serviciilor.
2. Respectarea principiilor GDPR privind prelucrarea datelor.
3. Documentarea corectă a datelor, inclusiv fluxurile, destinatarii și măsurile de protecție aplicate.
4. Monitorizarea riscurilor asociate prelucrării datelor și implementarea măsurilor corective.

V. Domeniu de aplicare

Această procedură se aplică:

1. Tuturor compartimentelor și serviciilor din cadrul Serviciului de Ambulanță Județean Iași (S.A.J), inclusiv:

- Secretariat;
- Compartiment Resurse Umane;
- Compartiment Medical (Dispecerat, Echipaje de intervenție);
- Serviciul Achiziții;
- Compartiment Legislație Contencios;
- Serviciul Tehnic, Mișcare și Exploatare Auto;
- Compartiment Financiar-Contabil;
- Compartiment IT;
- Compartiment Statistică și Informatică;

VI. Evidența activităților de prelucrare a datelor cu caracter personal

În conformitate cu art. 30 din Regulamentul (UE) 2016/679, Serviciul de Ambulanță Județean Iași are obligația de a păstra o evidență clară și detaliată a tuturor activităților de prelucrare a datelor cu caracter personal desfășurate în cadrul compartimentelor și serviciilor sale.

Această evidență se concretizează prin **Registrul de evidență a activităților de prelucrare**, care constituie un instrument esențial pentru:

- demonstrarea responsabilității instituționale în materie de protecția datelor;
- documentarea temeiurilor legale și a scopurilor fiecărei prelucrări;
- susținerea activităților de audit intern și de control din partea autorităților de supraveghere;
- prevenirea riscurilor și asigurarea trasabilității datelor.

Fiecare compartiment din cadrul instituției are responsabilitatea de a contribui la întocmirea și actualizarea registrului cu informații precise referitoare la activitățile proprii de prelucrare. Coordonarea acestui proces revine responsabilului cu protecția datelor (DPO), care asigură uniformitatea, corectitudinea și actualizarea permanentă a datelor înscrise.

În cele ce urmează se prezintă structura și conținutul registrului, precum și modul în care acesta trebuie completat de către fiecare compartiment.

VI.1. Structura Registrului pentru Fiecare Compartiment

Fiecare compartiment completează registrul conform următoarelor categorii:

1. Nr. crt.
2. Compartimentul (de ex.: Secretariat, Resurse Umane).
3. Scopul prelucrării (descriere clară a motivului pentru care sunt colectate datele).
4. Tipurile de date colectate (date personale, sensibile etc.).
5. Persoanele vizate (categorii, ex.: angajați, pacienți, colaboratori).
6. Temei legal (articole din GDPR care justifică prelucrarea).

7. Durata stocării (în conformitate cu cerințele legale).
8. Destinatarii (ex.: autorități, colaboratori externi).
9. Locația stocării (fizică sau electronică).
10. Măsuri de securitate (tehnice, organizatorice).
11. Riscuri (descrierea riscurilor și soluțiilor de reducere).
12. Persoana responsabilă (din cadrul compartimentului).

Registrul privind evidența datelor cu caracter personal din cadrul Serviciului de Ambulanță Județean Iași, cuprinde raționamentul și cadrul juridic în baza căruia instituția colectează și prelucrează datele cu caracter personal. Aceasta este o secțiune importantă care reflectă respectarea reglementărilor legale și justificarea prelucrării datelor.

Importanța registrului:

a. **Demonstrarea conformității cu GDPR**: Includerea temeiurilor legale și a scopurilor corecte în registru este esențială pentru a demonstra că prelucrarea datelor se face în conformitate cu regulamentele GDPR.
b. **Claritate și transparență**: Permite autorităților de reglementare și persoanelor vizate să înțeleagă clar scopurile și temeiurile prelucrării datelor.
c. **Protecția drepturilor persoanelor vizate**: Asigură că prelucrarea datelor este justificată și se face în scopuri legitime, protejând astfel drepturile pacienților și ale altor persoane vizate

Aceste detalii contribuie la completarea corespunzătoare a registrului de prelucrare a datelor cu caracter personal și garantează respectarea reglementărilor GDPR în cadrul activităților desfășurate de un serviciu de ambulanță.

Conform **Regulamentului (UE) 2016/679 (GDPR)**, toate activitățile de prelucrare a datelor cu caracter personal trebuie să fie întemeiate pe un temei legal specific, iar scopul prelucrării trebuie să fie clar definit.

VII. Cadrul legal general - GDPR:

7.1. Legislație europeană

Regulamentul (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 (GDPR).

7.2. Legislație națională

1. **Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR** în România.
2. **Legea nr. 95/2006 privind reforma în domeniul sănătății**, cu modificările și completările ulterioare, care include obligații privind păstrarea confidențialității datelor pacienților.
3. **Legea nr. 46/2003 privind drepturile pacientului**, care reglementează drepturile pacienților, inclusiv dreptul la confidențialitate și protecția datelor personale.
4. **Ordinul Ministerului Sănătății nr. 1091/2006**, privind gestionarea documentelor și raportărilor în instituțiile de sănătate publică.
5. **Legea nr. 500/2002 privind finanțele publice**, în măsura în care datele personale sunt utilizate în procesul de gestionare financiară.
6. **Ordonanța de urgență nr. 88/2012** privind organizarea și funcționarea serviciilor de ambulanță și SMURD.
7. **Codul Muncii (Legea nr. 53/2003)**, care include prevederi referitoare la prelucrarea datelor angajaților.

7.3. Reglementări și standarde aplicabile

1. **Reglementări emise de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**, inclusiv obligațiile privind notificarea breșelor de securitate și auditarea activităților de prelucrare.
2. **Standardele de securitate IT aplicabile sistemelor informatice utilizate în cadrul serviciului de ambulanță.**

7.4. Principii generale GDPR aplicabile

Această procedură respectă următoarele principii fundamentale prevăzute de GDPR:

1. **Legalitate, echitate și transparență**: Datele cu caracter personal sunt prelucrate în baza unui temei legal clar și în mod transparent față de persoanele vizate.
2. **Limitarea scopului**: Datele sunt colectate exclusiv pentru scopurile specificate, cum ar fi gestionarea intervențiilor, raportările statistice sau obligațiile legale.
3. **Reducerea la minimum a datelor**: Se colectează doar datele necesare pentru îndeplinirea scopurilor definite.
4. **Exactitate**: Datele sunt păstrate actualizate și corecte, cu mecanisme de corectare atunci când este necesar.
5. **Limitarea stocării**: Datele sunt păstrate numai pentru perioada prevăzută de lege sau necesară pentru scopurile prelucrării.
6. **Integritate și confidențialitate**: Se asigură măsuri adecvate pentru protecția datelor împotriva accesului neautorizat, pierderii sau distrugerii accidentale.

7.5. Drepturile persoanelor vizate

În cadrul Serviciului de Ambulanță Județean Iași (SAJ), sunt respectate toate drepturile persoanelor vizate în conformitate cu dispozițiile **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.

7.5.1. Dreptul la informare și acces la datele personale

(Art. 13, 14 și 15 din GDPR)

Persoanele vizate au dreptul:

- să primească informații clare, transparente și ușor de înțeles despre modul în care sunt colectate și utilizate datele lor cu caracter personal;
- să obțină confirmarea că datele lor sunt sau nu prelucrate;
- să aibă acces la datele proprii deținute de SAJ, inclusiv la scopul prelucrării, categoriile de date, destinatarii sau perioada stocării.

Aplicabil în SAJ: la momentul colectării datelor (de ex., la preluarea unui apel 112 sau în cadrul intervenției medicale), pacientul sau reprezentantul legal este informat cu privire la scopul și temeiul legal al prelucrării.

7.5.2. Dreptul la rectificarea datelor

(Art. 16 din GDPR)

Persoana vizată are dreptul:

- să solicite corectarea datelor inexacte sau completarea celor incomplete care o privesc, fără întârzieri nejustificate.

Aplicabil în SAJ IAȘI: rectificările pot fi operate în baza cererii scrise a persoanei vizate, după verificarea identității și a temeiului solicitării, în fișele de intervenție, registrele electronice sau alte evidențe medicale.

7.5.3. Dreptul la ștergerea datelor („dreptul de a fi uitat")

(Art. 17 din GDPR)

Acest drept permite ștergerea datelor cu caracter personal atunci când:

- datele nu mai sunt necesare în scopul pentru care au fost colectate;
- persoana vizată își retrage consimțământul (dacă prelucrarea s-a bazat pe consimțământ);
- datele au fost prelucrate ilegal.

Excepție importantă în SAJ IAȘI: acest drept **nu se aplică** atunci când prelucrarea este necesară pentru respectarea unei obligații legale sau pentru motive de interes public în domeniul sănătății publice – conform art. 17 alin. (3) lit. b și c din GDPR.

7.5.4. Dreptul la restricționarea prelucrării

(Art. 18 din GDPR)

Persoana vizată poate solicita restricționarea prelucrării dacă:

- contestă exactitatea datelor;
- prelucrarea este ilegală și persoana nu dorește ștergerea, ci doar limitarea;
- SAJ nu mai are nevoie de date, dar acestea sunt necesare persoanei vizate pentru apărarea unui drept;
- persoana se opune prelucrării, pe durata verificării prevalenței intereselor legitime.

Aplicabil în SAJ IAȘI: în perioada restricției, datele sunt păstrate dar nu prelucrate, cu excepția stocării sau pentru apărarea unui drept legal.

7.5.5. Dreptul la portabilitatea datelor

(Art. 20 din GDPR)

Persoana vizată are dreptul:

- să primească datele furnizate către SAJ într-un format structurat, utilizat în mod curent și care poate fi citit automat;
- să solicite transmiterea acestor date către un alt operator, dacă prelucrarea se bazează pe consimțământ sau pe un contract și se face prin mijloace automate.

Limitare în SAJ IAȘI: de regulă, acest drept este aplicabil limitat, întrucât prelucrarea datelor în domeniul medical se face în baza obligațiilor legale și a interesului public.

7.5.6. Dreptul la opoziție

(Art. 21 din GDPR)

Persoana vizată are dreptul:

- să se opună, din motive legate de situația sa particulară, prelucrării datelor personale efectuate în temeiul interesului public sau interesului legitim.

Aplicabil în SAJ Iași: dacă interesul public justifică prelucrarea (de exemplu, în caz de urgență medicală sau epidemii), cererea de opoziție poate fi respinsă cu motivare.

7.5.7. Dreptul de a depune o plângere la autoritatea de supraveghere

(Art. 77 din GDPR)

Persoana vizată are dreptul:

- să depună o plângere la **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**, dacă consideră că prelucrarea datelor sale s-a făcut ilegal sau cu încălcarea drepturilor.

Date de contact ANSPDCP:
Bd. G-ral Gheorghe Magheru 28-30, Sector 1, București
Email: anspdcp@dataprotection.ro
Website: www.dataprotection.ro

Modalitatea de exercitare a drepturilor

7.6. Modalități de transmitere a cererilor

Persoanele vizate pot transmite cereri:

- în format fizic (scris) – depusă la sediul SAJ, registratură;
- prin poștă cu confirmare de primire;
- prin e-mail la adresa oficială a DPO: **[introdu email DPO]**;
- prin intermediul unui formular tipizat pus la dispoziție de SAJ.

7.7. Verificarea identității

Pentru protejarea datelor, SAJ este îndreptățit să solicite:

- un document de identificare (copie CI, dacă cererea e în scris);
- date suplimentare pentru confirmarea identității în cazul solicitărilor online.

7.8. Termene de răspuns

- Termen standard: **cel mult 30 de zile** calendaristice de la primirea cererii.
- Dacă cererea este complexă: termenul poate fi prelungit cu maximum **două luni**, cu informarea prealabilă a persoanei vizate și justificarea întârzierii.

7.9. Evaluarea cererii

DPO, împreună cu compartimentele implicate (juridic, IT, medical etc.), analizează:

- temeiul legal al cererii;
- aplicabilitatea dreptului invocat;
- existența excepțiilor prevăzute de GDPR (ex: interes public, obligație legală etc.);
- impactul asupra datelor altor persoane.

7.10. Comunicarea răspunsului

Răspunsul se transmite:

- în aceeași modalitate în care a fost primită cererea (dacă nu se solicită altfel);
- într-un limbaj clar, concis și accesibil.

Dacă cererea este respinsă, se oferă:

- justificarea refuzului;
- menționarea dreptului de a depune plângere la ANSPDCP.

7.11. Evidența cererilor

Se păstrează un **Registru al cererilor GDPR**, ce va cuprinde:

- numărul de înregistrare;
- data primirii;
- numele solicitantului;
- tipul dreptului invocat;
- măsurile adoptate;
- data răspunsului;
- semnătura responsabilului.

Temeiuri legale pentru prelucrarea datelor(Articolul 6):

Prelucrarea datelor în cadrul Serviciului de Ambulanță Județean Iași se bazează pe:

1. **Obligații legale**: Prevederi impuse de legislația din domeniul sănătății și serviciilor de urgență.
2. **Interesul public major**: Gestionarea urgențelor medicale și intervențiilor rapide.
3. **Consimțământul persoanelor vizate**: Pentru prelucrarea anumitor categorii de date, atunci când nu există alt temei legal.

Articolul 6 (1) din GDPR stabilește cele șase temeiuri legale care permit prelucrarea datelor cu caracter personal:

a. **Consimțământul persoanei vizate** (litera a):
   - Prelucrarea datelor se poate face atunci când persoana vizată a dat consimțământul explicit pentru una sau mai multe scopuri specifice.
   - Ex: Consimțământul unui pacient pentru a procesa informațiile sale de sănătate pentru un tratament medical.

b. **Executarea unui contract** (litera b):
   - Prelucrarea datelor este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri înainte de încheierea unui contract.
   - Ex: Prelucrarea datelor angajaților pentru a le oferi salariul sau pentru administrarea beneficiilor.

c. **Îndeplinirea unei obligații legale** (litera c):
   - Prelucrarea este necesară pentru îndeplinirea unei obligații legale a operatorului.
   - Ex: În cadrul unui serviciu de ambulanță, prelucrarea datelor pentru raportarea unui incident medical autorităților (ex. autorităților de sănătate publică) sau pentru îndeplinirea obligațiilor fiscale.

d. **Protecția intereselor vitale ale persoanei vizate sau ale altor persoane fizice** (litera d):
   - Prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale altora.
   - Ex: Prelucrarea datelor personale ale unei persoane aflate într-o stare de urgență medicală, în vederea acordării unui tratament de urgență.

e. **Îndeplinirea unei sarcini de interes public sau în exercitarea unei autorități publice** (litera e):
   - Prelucrarea datelor este necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea unei autorități publice.
   - Ex: Prelucrarea datelor în scopuri legate de sănătatea publică sau pentru gestionarea serviciilor de urgență.

f. **Interesele legitime ale operatorului sau ale unei terțe părți** (litera f):
   - Prelucrarea este necesară pentru scopurile intereselor legitime urmărite de SAJ IASI sau de o terță parte, cu excepția cazului în care drepturile și libertățile fundamentale ale persoanei vizate prevalează.

Ex: Prelucrarea datelor angajaților pentru evaluarea performanței

VIII. Responsabilități

8.1.Responsabilul cu Protecția Datelor (DPO):

- Monitorizează aplicarea prevederilor GDPR și a procedurii operaționale.
- Evaluează periodic Registrul de Evidență a Datelor cu Caracter Personal.
- Informează conducerea asupra riscurilor și neconformităților identificate.

8.2. Șefii de compartimente și servicii:

- Asigură completarea și actualizarea periodică a registrului pentru activitățile din aria lor de competență.

- Aplică măsurile de protecție stabilite pentru datele prelucrate.

8.3. Persoanele desemnate din cadrul compartimentelor:

- Realizează evidența activităților de prelucrare a datelor.
- Răspund de corectitudinea și acuratețea informațiilor înregistrate.

8.4. Angajații:

- Respectă instrucțiunile de prelucrare a datelor stabilite prin această procedură.
- Informează imediat superiorii sau DPO-ul în cazul identificării unei posibile breșe de securitate.

IX. Definiții și Termeni Utilizați

1. **Date cu caracter personal**
   Orice informație referitoare la o persoană fizică identificată sau identificabilă, cum ar fi nume, adresă, CNP, date medicale, număr de telefon, adresă IP, locație GPS etc.
2. **Categorii speciale de date**
   Date care necesită o protecție suplimentară, cum ar fi:
   - Date privind starea de sănătate;
   - Date biometrice (ex.: amprente, scanări faciale);
   - Date genetice;
   - Apartenența religioasă, etnică, politică sau sindicală.
3. **Prelucrarea datelor**
   Orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal, inclusiv colectarea, stocarea, organizarea, utilizarea, modificarea, ștergerea sau transmiterea acestora.

4. **Operator de date**

Persoana juridică (în acest caz, Serviciul de Ambulanță Județean) care stabilește scopurile și mijloacele prelucrării datelor cu caracter personal.

5. **Persoană împuternicită de operator**

Persoana fizică sau juridică care prelucrează datele cu caracter personal în numele operatorului.

6. **Persoană vizată**

Orice persoană fizică ale cărei date personale sunt prelucrate, cum ar fi:

- Pacienții serviciului de ambulanță;
- Angajații SAJ;
- Colaboratorii și partenerii contractuali.

7. **Categorie destinatari**

Persoane fizice sau juridice, autorități publice, agenții sau alte organisme cărora le sunt divulgate datele cu caracter personal, cum ar fi:

- Spitale, pentru gestionarea cazurilor medicale;
- Casa Națională de Asigurări de Sănătate (CNAS);
- Organele de ordine publică sau autorități judiciare.

8. **Unde stocăm datele**

Mediul fizic sau electronic utilizat pentru păstrarea datelor, cum ar fi:

- Servere locale sau bazele de date electronice;
- Arhive fizice (dosare, registre);
- Platforme securizate de stocare.

9. **Cine intră în contact cu datele**

Persoanele autorizate să acceseze sau să prelucreze datele, inclusiv:

- Angajații din compartimentele implicate (statistică, dispecerat, echipaje medicale);
- Personalul IT responsabil cu mentenanța sistemelor;
- Persoanele desemnate prin procedură, în funcție de activitate.

10. **Risc**

Orice situație care ar putea compromite securitatea sau confidențialitatea datelor, cum ar fi:

- Accesul neautorizat;
- Pierderea sau furtul datelor;
- Erori umane sau breșe de securitate tehnologică.

11. **Persoana responsabilă la nivel de birou**

Angajat desemnat în fiecare compartiment sau serviciu pentru gestionarea corectă a datelor și asigurarea conformității activităților de prelucrare cu legislația aplicabilă și procedura.

12. **Măsuri de securitate**

Tehnici și proceduri aplicate pentru protejarea datelor, cum ar fi:

- Controlul accesului;
- Criptarea datelor sensibile;
- Backup-uri și planuri de continuitate operațională.

13. **Temei legal**

Justificarea pentru prelucrarea datelor, cum ar fi:

- Obligația legală a SAJ IAȘI;
- Consimțământul persoanei vizate;
- Executarea unui contract.

14. **Perioada de stocare a datelor**

Intervalul de timp pentru care datele sunt păstrate, stabilit conform legislației aplicabile sau necesităților operaționale.

15. **Breșă de securitate**

Incident care afectează confidențialitatea, integritatea sau disponibilitatea datelor, cum ar fi pierderea, accesul neautorizat sau coruperea datelor.

16. **Responsabil cu Protecția Datelor (DPO)**

Persoana desemnată să monitorizeze aplicarea regulamentului GDPR, să ofere consiliere instituției și să fie punct de contact pentru persoanele vizate și autoritățile de supraveghere.

17. **Fluxul de date**

Circulația datelor între compartimente interne sau între SAJ și destinatarii externi, cum ar fi autoritățile sau partenerii contractuali.

18. **Documente asociate**

Acte sau fișiere care sprijină procesul de prelucrare a datelor, cum ar fi fișele medicale, rapoartele statistice sau tabelele de evidență.

19. **Confidențialitate**

Principiul care asigură că datele sunt accesibile doar persoanelor autorizate și utilizate exclusiv pentru scopurile definite.

20. Operatori asociați

Este situația în care două sau mai multe entități (operatori) decid împreună scopurile și mijloacele prelucrării datelor. Fiecare operator are responsabilități clare în cadrul procesului de prelucrare a datelor.

X. Prelucrarea datelor sensibile (Articolul 9):

Conform Articolului 9 din GDPR, datele sensibile includ:

- **Originea rasială sau etnică.**
- **Opiniile politice.**
- **Convingerile religioase sau filosofice.**
- **Apartenența sindicală.**
- **Date genetice.**
- **Date biometrice** (pentru identificarea unică a unei persoane fizice).
- **Date privind sănătatea** (diagnostic, tratament, istoric medical).

- **Date privind viața sexuală sau orientarea sexuală.**

Principalele Reguli pentru Prelucrarea Datelor Sensibile

GDPR interzice prelucrarea datelor sensibile, cu excepția cazurilor în care se aplică cel puțin una dintre derogările specificate în Articolul 9(2).

Cadrul Legal pentru Prelucrarea Datelor Sensibile

1. **Temeiuri Legale Relevante pentru Datele Sensibile**:
    - **Art. 9(2)(a)**: Consimțământ explicit al persoanei vizate.
    - **Art. 9(2)(b)**: Necesitatea prelucrării pentru respectarea obligațiilor în domeniul ocupării forței de muncă sau al securității sociale.
    - **Art. 9(2)(c)**: Protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane, atunci când aceasta este incapabilă să-și dea consimțământul.
    - **Art. 9(2)(h)**: Prelucrarea este necesară în scopuri de asistență medicală preventivă, diagnostic medical, furnizarea tratamentului medical.
    - **Art. 9(2)(i)**: Prelucrarea este necesară din motive de interes public, cum ar fi sănătatea publică.
2. **Art. 6 – Temei General**:
    - Pentru a prelucra datele sensibile, trebuie să existe și un temei general, cum ar fi:
        - Art. 6(1)(c): Îndeplinirea unei obligații legale.
        - Art. 6(1)(d): Protejarea intereselor vitale.
        - Art. 6(1)(e): Îndeplinirea unei sarcini de interes public sau care rezultă din exercitarea autorității publice.

Exemple de Prelucrare a Datelor Sensibile în Serviciul de Ambulanță

1. **În cadrul Compartimentului Medical**:
   - Colectarea și stocarea datelor despre diagnostic, tratament și istoricul medical al pacienților pentru furnizarea îngrijirilor medicale.
   - Trimiterea de rapoarte către autorități despre boli contagioase (interes public).
2. **În Dispecerat**:
   - Preluarea informațiilor despre simptomele pacientului și istoricul medical, dacă sunt comunicate de apelant.
3. **În cadrul Echipajelor de Intervenție**:
   - Notarea valorilor fiziologice (tensiune, puls, glicemie) în fișa de intervenție.
   - Colectarea datelor pentru diagnostic rapid și tratament pe teren.

Măsuri de Securitate pentru Datele Sensibile

1. **Măsuri Fizice**:
   - Păstrarea fișelor medicale în dulapuri securizate.
   - Restricționarea accesului la arhivele fizice.
2. **Măsuri Tehnice**:
   - Criptarea datelor stocate electronic.
   - Sisteme de acces bazate pe autentificare dublă (ex. parole și carduri).
3. **Măsuri Organizaționale**:
   - Instruirea personalului în privința GDPR și confidențialității.
   - Limitarea accesului la date doar pentru personalul autorizat.

Riscuri Asociate Prelucrării Datelor Sensibile

1. **Acces Neautorizat**:
   - Poate cauza expunerea informațiilor medicale sensibile, ducând la prejudicii pentru pacient.
2. **Pierderea sau Distrugerea Datelor**:
   - Poate afecta continuitatea tratamentului medical.
3. **Utilizarea Neadecvată a Datelor**:
   - Exemplu: divulgarea istoricului medical către terți fără consimțământ sau temei legal.

Prelucrarea datelor sensibile necesită o atenție deosebită datorită riscurilor mari implicate pentru drepturile și libertățile persoanei vizate. Este esențial ca toate procesele să fie conforme cu GDPR, să fie documentate în registrul de evidență și să includă măsuri stricte de securitate pentru protejarea acestor date

Concluzii importante:

1. **Transparența** – Registrul oferă o evidență clară a activităților de prelucrare a datelor, permițând persoanelor vizate să înțeleagă cum și de ce sunt procesate datele lor.
2. **Conformitatea** – Asigură respectarea cerințelor legale prevăzute de GDPR și alte reglementări relevante, cum ar fi protecția datelor sensibile.
3. **Control și Monitorizare** – Permite organizațiilor să controleze accesul și utilizarea datelor personale, reducând riscurile de abuzuri sau erori.
4. **Drepturile persoanelor vizate** – Oferă un cadru clar pentru exercitarea drepturilor acestora, cum ar fi dreptul de acces, rectificare, ștergere sau opoziție la prelucrarea datelor.

5. **Măsuri de securitate** – Este esențial să se stabilească și să se implementeze măsuri de securitate adecvate pentru protecția datelor, atât în format fizic, cât și electronic.
6. **Răspundere** – Fiecare compartiment și persoană implicată în procesul de prelucrare a datelor trebuie să fie responsabilă pentru respectarea principiilor GDPR.

În concluzie, registrul de prelucrare a datelor este un instrument vital pentru protecția datelor personale și pentru îndeplinirea obligațiilor legale ale instituției, contribuind la menținerea unui mediu sigur și conform în cadrul activităților de prelucrare a datelor cu caracter personal.

4. Documentarea cadrului legal în registru:

În secțiunea **„Cadrul legal"** din registrul de evidență a prelucrărilor de date cu caracter personal, trebuie menționat temeiul legal specific care permite prelucrarea fiecărei categorii de date. De asemenea, trebuie documentat scopul prelucrării în conformitate cu articolele menționate anterior.

Exemplu de completare:

Activitatea de prelucrare	**Cadrul legal**
Prelucrarea datelor pacienților (pentru administrarea tratamentului de prim ajutor)	Articolul 6 (1)(c) - Îndeplinirea unei obligații legale; Articolul 9 (2)(h) - Prelucrarea datelor pentru scopuri de asistență medicală.
Prelucrarea datelor angajaților	Articolul 6 (1)(b) - Executarea unui contract; Articolul 9 (2)(b) - Prelucrarea datelor pentru îndeplinirea obligațiilor legale în domeniul muncii.
Prelucrarea datelor pentru recrutarea de personal	Articolul 6 (1)(a) - Consimțământul persoanei vizate; Articolul 9 (2)(b) - Prelucrarea datelor pentru recrutare și selecție personală.

XI . Instrucțiuni specifice de completare a registrului pentru fiecare coloană din Registru de Evidență privind Prelucrare a Datelor cu Caracter Personal al S.A.J. Iași (Anexa 1)

În conformitate cu Regulamentul General privind Protecția Datelor (GDPR), Serviciul de Ambulanță Județean Iași (S.A.J) are obligația de a documenta în mod detaliat activitățile de prelucrare a datelor cu caracter personal. Registrul de Evidență a Prelucrării Datelor cu Caracter Personal al SAJ este un instrument esențial pentru asigurarea transparenței și conformității cu reglementările europene și naționale privind protecția datelor. Acesta facilitează monitorizarea și controlul activităților de prelucrare, contribuind la protejarea drepturilor persoanelor vizate și asigurarea unui management responsabil al datelor personale.

Registrul este structurat în 17 coloane, fiecare reflectând un aspect important al procesului de prelucrare a datelor. Completarea corectă a fiecărei coloane este esențială pentru asigurarea respectării principiilor GDPR, inclusiv transparența, legalitatea, exactitatea și minimizarea prelucrării datelor.

Capitolul „Instrucțiuni specifice de completare a registrului" din cadrul acestei proceduri operaționale oferă clarificări detaliate pentru fiecare coloană, având rolul de a ghida personalul responsabil în completarea corectă a registrului, conform cerințelor legale și interne. Prin urmare, este esențial ca fiecare coloană să fie completată cu informații precise și actualizate, pentru a asigura trasabilitatea și conformitatea proceselor de prelucrare a datelor personale.

Cele 17 coloane, descrise în detaliu în acest capitol, includ aspecte precum proveniența datelor, scopul prelucrării, temeiul legal, destinatarii datelor, măsurile de securitate și durata păstrării acestora. De asemenea, se vor preciza măsurile de protecție a datelor și persoanele responsabile la nivel de departament sau serviciu, pentru a asigura un control riguros asupra procesului de prelucrare.

Instrucțiunile specifice sunt destinate tuturor angajaților și persoanelor desemnate din cadrul SAJ care gestionează și prelucrează date personale, asigurând astfel un cadru coerent și transparent în activitățile de prelucrare a datelor cu caracter personal. Este esențial ca fiecare compartiment sau serviciu să cunoască responsabilitățile și obligațiile care îi revin în acest proces, pentru a proteja în mod eficient datele personale și pentru a respecta reglementările în vigoare.

XI.1. Coloana 1- Provenienta datelor/Surse

Tipuri de surse pentru datele prelucrate

În cadrul Serviciului de Ambulanță Județean Iași, datele cu caracter personal prelucrate în diverse compartimente și servicii provin din următoarele surse:

1. Persoane fizice direct vizate:

- Pacienți, aparținători, colaboratori, care transmit cereri, reclamații sau solicitări către instituție.
- Angajați care depun documente administrative (ex.: cereri de concediu, adeverințe, declarații).

2. Alte departamente interne:

- Date transmise de alte birouri sau departamente ale instituției.
    - **Exemple:** Date transmise de departamentul de resurse umane (dosare ale angajaților, adrese privind promovări, transformări, etc.).

3. Instituții terțe și autorități publice:

- Date primite prin corespondență oficială de la alte instituții publice (ex.: DSP, instanțe de judecată, alte autorități publice).

4. Platforme sau sisteme interne:

- Sisteme de management al documentelor (DMS) sau aplicații electronice utilizate pentru corespondență și gestiunea datelor (ex.: platforme electronice de raportare, aplicații de gestionare a solicitărilor online).

Observații importante pentru completare în Registrului:

- Pentru fiecare activitate de prelucrare, trebuie menționată clar sursa datelor personale în registru.
- Dacă datele provin de la terți (ex.: autorități publice, alte instituții), acest lucru trebuie justificat prin documentele relevante și inclus în registru. Documentele care atestă transferul datelor trebuie arhivate conform procedurilor interne.
- În cazul colectării de date prin mijloace digitale (ex.: platforme online), acest aspect trebuie specificat clar la categoria „Proveniența datelor/Surse".

XI.2. Coloana 2 – Categoria/tipul de date personale colectate

1. Date de identificare personală

- Nume și prenume.
- CNP (dacă este inclus în documentele oficiale).
- Serie și număr CI (dacă este relevant, ex.: pentru adeverințe).
- Semnătura (pe cereri, reclamații sau alte documente).

2. Date de contact

- Adresă de domiciliu/reședință (din cereri sau documente oficiale).
- Număr de telefon.
- Adresă de e-mail.

3. Date profesionale

- Funcția și locul de muncă (dacă este vorba despre angajați sau parteneri din alte instituții).
- Numărul matricol sau identificator unic în instituție (pentru personalul intern).

4. Date administrative și documentare

- Date incluse în cereri administrative (ex.: concedii, solicitări de adeverințe).
- Documente privind situații juridice (reclamații, solicitări de informații, alte proceduri oficiale).

5. Date speciale (categorii sensibile)

- **Date privind sănătatea** (în cazul în care pacienții adresează cereri sau documente ce conțin astfel de informații).
- **Date financiare** (ex.: salarii incluse în adeverințele emise pentru angajați).

6. Date din corespondență și comunicări

- Conținutul cererilor/reclamațiilor transmise către instituție.
- Alte informații personale incluse în documentele primite de la persoane fizice sau juridice.

Activitatea de prelucrare	**Tipuri de date colectate**
Gestionarea corespondenței	Nume, prenume, adresă, număr de telefon, e-mail, semnătura, conținutul solicitării

Arhivarea documentelor	Nume, prenume, CNP, semnătura, date incluse în documente administrative sau juridice
Evidența cererilor administrative	Nume, prenume, CNP, funcție, date privind sănătatea (dacă sunt incluse în cereri), date financiare (ex.: salarii)
Organizarea audiențelor	Nume, prenume, date de contact (telefon, e-mail), subiectul audienței

Principii de completare

1. **Exactitate și exhaustivitate**: Se înregistrează doar datele strict necesare pentru fiecare activitate.
2. **Minimizare**: Se evită colectarea unor date care nu sunt relevante pentru scopul activității.
3. Dacă datele sunt sensibile (ex.: sănătate), trebuie menționat clar temeiul legal al prelucrării în coloana 4(temei legal) și măsurile speciale de protecție în coloana 17

XI. Coloana 3 – Categorii de personae vizate (ale cui date colectăm?)

Categorii de persoane vizate:

1. **Angajați ai SAJ IAȘI**
   - Personalul administrativ.
   - Personalul medical (adeverințe, documente interne).
2. **Pacienți**
   - Persoanele care adresează cereri sau solicitări SAJ IASI (de exemplu, pentru informații, reclamații, solicitări de documente).
   - Persoane care interacționează cu secretariatul în contextul furnizării serviciilor de urgență prespitalicească.
3. **Persoane care depun cereri sau reclamații**
   - Orice persoană fizică care face o solicitare către SAJ IAȘI, cum ar fi cetățeni care cer informații sau depun plângeri/reclamații.

4. **Vizitatori ai SAJ IAȘI**
   - Persoane care vin pentru audiențe sau întâlniri la instituție și își lasă datele de contact.
5. **Colaboratori externi sau parteneri**
   - Avocați, consultanți, furnizori de servicii care pot fi înregistrați în sistemul instituției pentru diverse activități administrative.
6. **Reprezentanți ai altor instituții publice sau private**
   - Persoane care contactează instituția în numele unor organizații externe, cum ar fi autoritățile locale, DSP, instanțele de judecată etc.
7. **Alți terți**
   - Orice terț care are o relație administrativă sau contractuală cu instituția (ex.: persoane care transmit documente oficiale, avize sau alte comunicări).

Detalii suplimentare pentru completare

1. **Claritatea categoriilor**: Este important ca, în funcție de activitățile specifice, să fie identificate exact categoriile de persoane vizate. De exemplu, în cazul gestionării corespondenței, nu sunt doar pacienți și angajați, ci și reprezentanți ai altor instituții care pot trimite documente.
2. **Includerea tuturor categoriilor relevante**: De exemplu, dacă secretariatul gestionează audiențe pentru alte persoane (ex.: cetățeni, consultanți, reprezentanți legali), toate aceste grupuri trebuie specificate.
3. **Confidențialitatea**: Este esențial să se menționeze toate categoriile de persoane, inclusiv persoanele fizice ale căror date pot fi colectate accidental sau ocazional (de exemplu, în cazul reclamațiilor sau întâlnirilor informale).

XI.4 Coloana 4- Temeiul legal

În coloana **„Temeiul legal"** din registrul de prelucrare a datelor cu caracter personal, trebuie indicată baza legală care justifică prelucrarea datelor, conform articolului 6 din GDPR. În funcție de activitatea desfășurată de secretariatul instituției, se aplică una sau mai multe dintre următoarele temeiuri legale:

Temeiuri legale comune în cazul secretariatului:

- **Art. 6 alin. 1 lit. c GDPR: Obligația legală**
  Se aplică atunci când prelucrarea este necesară pentru a respecta obligațiile legale ale instituției.

Exemple:

Gestionarea corespondenței oficiale.
Arhivarea documentelor conform legislației aplicabile (ex.: Legea Arhivelor Naționale).
Emiterea documentelor oficiale (adeverințe, răspunsuri la cereri).

- **Art. 6 alin. 1 lit. e GDPR: Interesul public**
  Este utilizat pentru activitățile ce implică furnizarea serviciilor publice sau exercitarea atribuțiilor oficiale.

Exemple: Răspunsuri la solicitări publice sau administrative.

Organizarea audiențelor pentru persoane fizice.

- **Art. 6 alin. 1 lit. a GDPR: Consimțământul persoanei vizate**
  Se aplică pentru activități în care datele sunt prelucrate cu acordul explicit al persoanei.

Exemple:

Procesarea unor cereri care nu sunt obligatorii din punct de vedere legal (ex.: eliberarea unor informații suplimentare la cerere).

- **Art. 6 alin. 1 lit. b GDPR: Executarea unui contract**
  Se poate aplica în situații unde există o relație contractuală între persoana vizată și instituție.

Exemple:

Gestionarea documentelor administrative ale angajaților, în cadrul relației de muncă.

- **Art. 6 alin. 1 lit. d GDPR: Interesul vital al persoanei vizate**
  În situații rare, datele pot fi prelucrate pentru protejarea intereselor vitale ale unei persoane, de exemplu, în caz de urgențe medicale.

Exemplu de completare in registru:

Activitatea de prelucrare	**Temeiul legal**
Gestionarea corespondenței	Art. 6 alin. 1 lit. c GDPR – Obligația legală (Legea nr. 544/2001 privind liberul acces la informații publice)
Arhivarea documentelor	Art. 6 alin. 1 lit. c GDPR – Obligația legală (Legea Arhivelor Naționale nr. 16/1996)
Evidența cererilor administrative	Art. 6 alin. 1 lit. c GDPR – Obligația legală (Codul Muncii,)
Organizarea audiențelor	Art. 6 alin. 1 lit. e GDPR – Interes public
Procesarea cererilor voluntare	Art. 6 alin. 1 lit. a GDPR – Consimțământ

Aspecte importante pentru completarea temeiului legal

1. **Corelarea temeiului legal cu activitatea specifică:** Fiecare activitate de prelucrare trebuie să aibă un temei clar justificat.
2. **Specificarea legislației aplicabile:** În cazul obligațiilor legale, se pot menționa actele normative relevante (ex.: Codul Muncii,etc) 3.
3. **Documentare suplimentară:** Consimțământul persoanei vizate trebuie documentat (ex.: formulare de consimțământ semnate).

XI.5.Coloana 5 – Destinatarii (cui sunt adresate/dezvăluite/ transmise ?)

In coloana **„Categorii de destinatari"** din registrul de prelucrare a datelor cu caracter personal, trebuie menționate entitățile interne sau externe care primesc sau ar putea primi acces la datele prelucrate. Această secțiune este esențială pentru a documenta transparența procesului de partajare a datelor și pentru respectarea articolelor 13 și 14 din GDPR.

Destinatarii posibili în cazul secretariatului Serviciului de Ambulanță

1. Destinatari interni (din cadrul instituției)

Aceștia sunt entități sau compartimente/departamente/servicii/birouri care au acces la date în contextul activităților administrative:

- **Departamentul Resurse Umane**: pentru gestionarea cererilor administrative sau a documentelor angajaților.
- **Departamentul Financiar-Contabil**: pentru date incluse în documentele legate de salarii sau alte beneficii.
- **Departamentul Medical**: pentru informații relevante despre pacienți, dacă este cazul.
- **Managerul instituției**: în cazul documentelor legate de activitățile de raportare.

2. Destinatari externi (entități din afara instituției)

Aceștia sunt autorități, parteneri sau alte entități care primesc date în conformitate cu obligațiile legale sau contractuale:

- **Autorități publice**:
  - Direcția de Sănătate Publică (DSP), IGSU, DSU,MS, Prefectură, CJ
  - Casele de asigurări de sănătate (în cazul solicitărilor administrative).
  - Instanțele de judecată sau alte autorități juridice (în cazul litigiilor).

- **Arhive naționale sau furnizori de servicii de arhivare**: dacă datele sunt transmise pentru arhivare conform legii.
- **Furnizori de servicii IT**: dacă baza de date sau documentele sunt gestionate printr-o platformă externă.
- **Reprezentanți legali**: în cazul procedurilor juridice care necesită acces la date.

3. Alte categorii de destinatari

- **Persoanele vizate însele**: Dacă acestea solicită acces la propriile date în conformitate cu drepturile lor (art. 15 GDPR).
- **Parteneri contractuali**: de exemplu, firme de audit sau consultanță, furnizori

Aspecte importante pentru completare, privind destinatarii

1. **Claritatea și specificitatea destinatarilor:** Menționează destinatarii atât generici (de exemplu, autorități publice), cât și cei specifici (ex.: DSP, instanțe).
2. **Justificarea transmiterii datelor către destinatari externi:** Este esențial ca, pentru fiecare destinatar, să existe o justificare documentată (ex.: obligație legală, interes public).
3. **Limitarea accesului:** Se specifică doar destinatarii care au nevoie de date pentru un scop legitim și justificat.

XI.6. Coloana 6 - Scopul prelucrării datelor cu caracter personal

Scopul Prelucrării Datelor cu Caracter Personal

Prelucrarea datelor cu caracter personal în cadrul Serviciului de Ambulanță Județean Iași (SAJ) se realizează în scopuri clare, legitime și conforme cu legislația în vigoare. Activitatea de prelucrare a datelor este esențială pentru buna desfășurare a misiunilor specifice ale instituției, respectând principiile stabilite de Regulamentul General privind Protecția Datelor (GDPR). Fiecare activitate de prelucrare trebuie să aibă un scop bine definit și justificat.

PROCEDURĂ OPERAȚIONLĂ

Prelucrarea Datelor cu Caracter Personal în cadrul Serviciului de Ambulanță Județean Iași

GDPR

1. Gestionarea cazurilor de urgență și intervenții medicale

- **Scopul prelucrării:** Colectarea și procesarea datelor pacienților (inclusiv datele sensibile, cum ar fi starea de sănătate) în vederea prestării serviciilor de urgență medicală.
- **Activități:** Identificarea pacienților, evaluarea stării acestora, stabilirea intervenției corespunzătoare și transmiterea informațiilor către echipele de intervenție.
- **Justificare:** Aceste activități sunt necesare pentru furnizarea corectă și promptă a serviciilor de urgență, în conformitate cu legislația națională și cu reglementările medicale aplicabile.

2. Gestionarea relațiilor cu pacienții și familiile acestora

- **Scopul prelucrării:** Procesarea cererilor, reclamațiilor și solicitărilor legate de serviciile prestate, inclusiv urmărirea stării de sănătate post-intervenție.
- **Activități:** Înregistrarea și procesarea sesizărilor din partea pacienților sau a familiilor acestora, furnizarea de răspunsuri oficiale, și îmbunătățirea continuă a serviciilor oferite.
- **Justificare:** Scopul prelucrării este conform cu obligațiile legale și etice de a îmbunătăți serviciile de sănătate și de a proteja interesele pacienților.

3. Gestionarea documentelor administrative și corespondenței oficiale

- **Scopul prelucrării:** Organizarea și arhivarea documentelor administrative și oficiale (solicitări, cereri, reclamații, etc.), conform cerințelor legale.
- **Activități:** Procesarea documentelor primite și expediate, inclusiv întocmirea răspunsurilor către autorități sau alte instituții.
- **Justificare:** Aceste activități sunt necesare pentru conformitatea cu reglementările legale, inclusiv Legea nr. 544/2001 privind accesul la informațiile de interes public.

4. Arhivarea și gestionarea documentației pacientului

- **Scopul prelucrării:** Păstrarea în siguranță a documentelor pacientului și a istoricului medical.
- **Activități:** Crearea și actualizarea dosarelor pacientului, arhivarea acestora în conformitate cu normele legale privind protecția datelor și gestionarea documentelor medicale.
- **Justificare:** Aceasta este o activitate necesară pentru continuitatea îngrijirii pacientului și pentru respectarea reglementărilor privind stocarea și accesul la informațiile medicale.

5. Suport administrativ pentru alte departamente

- **Scopul prelucrării:** Furnizarea de date administrative și informații interne către diverse departamente, cum ar fi resurse umane, financiar-contabil și medical.
- **Activități:** Colectarea și transmiterea datelor relevante pentru procesarea cererilor angajaților (de exemplu, cereri de concediu, adeverințe, documente financiare).
- **Justificare:** Aceste activități sunt necesare pentru funcționarea eficientă a instituției și pentru îndeplinirea obligațiilor administrative.

6. Conformitatea cu reglementările legale

- **Scopul prelucrării:** Asigurarea respectării reglementărilor legale aplicabile, inclusiv GDPR, Legea nr. 544/2001 și alte reglementări specifice sectorului medical.
- **Activități:** Monitorizarea respectării normelor legale privind protecția datelor cu caracter personal, gestionarea cererilor de acces la informații și implementarea măsurilor de conformitate.
- **Justificare:** Prelucrarea datelor în acest scop este necesară pentru a îndeplini obligațiile legale ale instituției.

7. Gestionarea și îmbunătățirea proceselor de instruire și evaluare

- **Scopul prelucrării:** Colectarea datelor legate de formarea și evaluarea personalului.
- **Activități:** Înregistrarea și actualizarea informațiilor referitoare la instruirea personalului, evaluarea performanțelor și gestionarea proceselor de feedback.
- **Justificare:** Scopul prelucrării este necesar pentru gestionarea eficientă a resurselor umane și pentru îmbunătățirea calității serviciilor prestate.

8. Protecția și securitatea datelor

- **Scopul prelucrării:** Asigurarea securității și protecției datelor cu caracter personal în cadrul activității SAJ.
- **Activități:** Implementarea măsurilor tehnice și organizatorice pentru protecția datelor (de exemplu, criptarea, backup-urile, autentificarea multi-factor).
- **Justificare:** Activitățile sunt necesare pentru a preveni riscurile legate de securitatea datelor și pentru a respecta reglementările GDPR privind protecția datelor.

9. Gestionarea incidentelor de securitate

- **Scopul prelucrării:** Detectarea și gestionarea incidentelor de securitate, inclusiv breșe de securitate și atacuri cibernetice.
- **Activități:** Colectarea și analizarea datelor legate de incidentele de securitate și implementarea măsurilor corective.
- **Justificare:** Aceste activități sunt necesare pentru prevenirea și minimizarea impactului asupra datelor cu caracter personal și pentru respectarea reglementărilor privind securitatea cibernetică.

Aspecte Importante pentru Completarea Registrului

1. **Scopuri clare și legitime:** Fiecare activitate de prelucrare a datelor trebuie să aibă un scop clar definit și justificat. Scopurile trebuie să fie specifice și să nu fie vagi sau generice (de exemplu, „pentru utilizare internă").
2. **Conformitate cu legislația:** Scopul prelucrării trebuie să fie conform cu obligațiile legale impuse de legislația națională și europeană.
3. **Prevenirea prelucrărilor incompatibile:** Datele nu trebuie să fie prelucrate în scopuri care nu sunt compatibile cu scopurile pentru care au fost colectate, cu excepția cazurilor prevăzute de lege sau reglementări specifice.

Exemple de completare a registrului (în cazul activității de secretariat) privind scopul prelucrării datelor cu caracter personal

Activitatea de prelucrare	Scopul prelucrării
Gestionarea corespondenței	Procesarea solicitărilor și reclamațiilor oficiale, transmiterea răspunsurilor către autorități sau persoane fizice
Arhivarea documentelor	Păstrarea documentelor administrative și oficiale în conformitate cu legislația privind arhivarea
Evidența cererilor administrative	Gestionarea cererilor legate de concedii, adeverințe, sau alte solicitări administrative
Organizarea audiențelor	Planificarea și desfășurarea întâlnirilor oficiale între cetățeni și conducerea instituției
Emiterea documentelor oficiale	Eliberarea adeverințelor, confirmărilor sau răspunsurilor oficiale către angajați, pacienți sau alte persoane fizice

Aspecte importante pentru completare

1. **Scopurile trebuie să fie clare și detaliate:** Evită formulările generale (ex.: „pentru utilizare internă") și specifică exact motivul prelucrării.
2. **Scopurile să fie compatibile cu legislația:** Toate scopurile trebuie să fie conforme cu legile naționale și internaționale aplicabile.

3. **Scopuri secundare:** Dacă există scopuri adiționale (ex.: cercetare), acestea trebuie clar evidențiate, iar prelucrarea să fie efectuată doar dacă este permisă legal.

Articole relevante din GDPR pentru activitățile de secretariat

1. **Articolul 6(1)(c) – Obligația legală**
   - Activitatea de secretariat implică adesea prelucrarea datelor în baza obligațiilor legale pe care instituția trebuie să le respecte.
   - Exemple:
     - Gestionarea corespondenței oficiale (Legea nr. 544/2001 privind accesul la informații de interes public).
     - Arhivarea documentelor conform legislației arhivistice (Legea Arhivelor Naționale).
     - Emiterea de documente administrative (adeverințe, răspunsuri oficiale).
2. **Articolul 6(1)(e) – Interesul public**
   - Prelucrarea datelor de către serviciile de ambulanță, inclusiv secretariatul, este justificată prin faptul că aceste activități sunt realizate pentru îndeplinirea unei sarcini de interes public sau care rezultă din exercitarea autorității publice cu care este învestită instituția.
   - Exemple:
     - Gestionarea reclamațiilor pacienților sau cetățenilor.
3. **Articolul 6(1)(b) – Executarea unui contract**
   - Dacă secretariatul gestionează cereri legate de contractele de muncă (de exemplu, adeverințe pentru angajați), acest temei poate fi aplicabil.
4. **Articolul 6(1)(f) – Interesul legitim**
   - În anumite cazuri, prelucrarea poate fi justificată prin interesul legitim al instituției, cu condiția ca acest interes să nu prevaleze asupra drepturilor și libertăților persoanelor vizate.
   - Exemple:

- Asigurarea securității documentelor și a informațiilor sensibile prin arhivare și organizare adecvată.
- Supravegherea video a zonei administrative pentru prevenirea accesului neautorizat, protejarea bunurilor și a echipamentelor.

5. **Articolul 9(2)(h) – Prelucrarea datelor sensibile în scopuri medicale** *(în cazuri specifice)*
   - În cazul în care secretariatul prelucrează informații medicale pentru gestionarea cazurilor (de exemplu, reclamații sau solicitări ale pacienților), acest articol poate fi aplicabil.

Exemple de justificare în registru pentru activitatea de secretariat

Activitatea de prelucrare	Scopul prelucrării	Temei legal
Gestionarea corespondenței	Gestionarea solicitărilor și reclamațiilor oficiale	Art. 6(1)(c) – Obligația legală; Art. 6(1)(e) – Interes public
Organizarea audiențelor	Planificarea și desfășurarea întâlnirilor oficiale	Art. 6(1)(e) – Interes public
Arhivarea documentelor	Păstrarea documentelor administrative conform legii	Art. 6(1)(c) – Obligația legală
Emiterea documentelor oficiale	Eliberarea adeverințelor sau altor documente solicitate	Art. 6(1)(b) – Executarea unui contract (angajați); Art. 6(1)(c) – Obligația legală
Supravegherea video	Asigurarea securității informațiilor și documentelor	Art. 6(1)(f) – Interes legitim

XI.7. Coloana 7„Cum prelucrăm datele (hârtie/format electronic)"

În coloana **„Cum prelucrăm datele (hârtie/format electronic)"**, trebuie să specificați formatul în care datele cu caracter personal sunt gestionate, stocate și utilizate de către secretariatul instituției. Este important să menționați dacă prelucrarea se face pe suport fizic (hârtie) sau digital (format electronic) sau ambele, pentru a evidenția procesele implicate.

Ghid detaliat pentru completarea coloanei „Cum prelucrăm datele (hârtie/format electronic)" în registrul de evidență a prelucrării datelor

Pentru fiecare activitate desfășurată de secretariat, trebuie să detaliați clar modul în care sunt gestionate datele cu caracter personal. Ghidul de mai jos oferă explicații și exemple adaptate activităților uzuale ale unui secretariat dintr-un serviciu de ambulanță.

1. Gestionarea corespondenței oficiale

- **Procesul:**
  - Solicitările sau răspunsurile scrise primite de la instituții, pacienți, angajați sau alte părți interesate sunt înregistrate.
  - Corespondența este redactată și transmisă fie în format fizic (hârtie), fie electronic (e-mail).
- **Cum prelucrăm datele:**
  - **Hârtie:** Solicitările primite în format fizic, registrele de intrări/ieșiri.
  - **Format electronic:** Corespondența redactată, trimisă sau primită prin e-mail, stocată în sistemele informatice.

2. Emiterea adeverințelor pentru angajați

- **Procesul:**
  - Angajații pot solicita adeverințe (pentru medic, bancă, etc.). Informațiile sunt prelucrate în format electronic pentru redactare, apoi documentele sunt tipărite.
- **Cum prelucrăm datele:**
  - **Format electronic:** Crearea documentului (Microsoft Word, sisteme informatice).
  - **Hârtie:** Adeverințele tipărite, semnate și arhivate în dosarul personal al angajatului.

3. Înregistrarea cererilor și reclamațiilor

- **Procesul:**
  - Cetățenii sau alte părți interesate depun cereri sau reclamații în format fizic sau electronic. Secretariatul le înregistrează și le transmite către departamentele responsabile.
- **Cum prelucrăm data:**
  - **Hârtie:** Reclamații/cereri scrise depuse personal sau prin poștă.
  - **Format electronic:** Reclamații/cereri primite prin e-mail sau portaluri online; înregistrarea acestora într-un sistem informatic.

4. Arhivarea documentelor

- **Procesul:**
  - Documentele administrative (adeverințe, corespondență, cereri, rapoarte) sunt stocate conform unei politici de arhivare.
- **Cum prelucrăm datele:**
  - **Hârtie:** Păstrarea documentelor fizice în arhive sau dulapuri securizate.
  - **Format electronic:** Scanarea documentelor și stocarea acestora pe servere securizate sau în sisteme de arhivare electronică.

5. Răspunsuri către autorități sau cetățeni

- **Procesul:**
  - Secretariatul gestionează cererile oficiale din partea autorităților (ex.: DSP, ITM) sau răspunsurile adresate pacienților.
- **Cum prelucrăm datele:**
  - **Hârtie:** Solicitări sau răspunsuri trimise prin poștă sau depuse fizic.
  - **Format electronic:** Redactarea și transmiterea răspunsurilor prin e-mail; păstrarea acestora în sistemele informatice.

6. Gestionarea dosarelor de personal

- **Procesul:**
  - Secretariatul poate colabora cu departamentul de resurse umane pentru gestionarea datelor angajaților (adeverințe, dosare de personal).
- **Cum prelucrăm datele:**
  - **Hârtie:** Dosare fizice ale angajaților, inclusiv cereri, contracte și alte documente tipărite.
  - **Format electronic:** Baze de date privind angajații, adeverințe redactate pe computer.

7. Supravegherea video a spațiilor administrative

- **Procesul:**
  - Zonele administrative sunt monitorizate pentru asigurarea securității datelor și spațiilor.
- **Cum prelucrăm datele:**
  - **Format electronic:** Înregistrările video sunt stocate pe servere securizate, accesibile doar persoanelor autorizate.

8. Organizarea audiențelor

- **Procesul:**
  - Secretariatul înregistrează programările și detaliile privind persoanele care solicită audiențe.
- **Cum prelucrăm datele:**
  - **Hârtie:** Cereri scrise de programare, registre pentru evidența audiențelor.
  - **Format electronic:** Programarea audiențelor în calendare electronice sau sisteme de management.

XI.8. Coloana 8 „Categorii de destinatari"

În coloana **„Categorie destinatari (interni/externi)"** trebuie să specificați către cine sunt transmise sau împărtășite datele cu caracter personal prelucrate de secretariat. Această coloană evidențiază tipul de destinatari și clasificarea lor, fie în cadrul organizației (interni), fie în afara acesteia (externi).

Definiții și exemple pentru destinatari:

1. **Destinatari interni:**
   - Persoane sau departamente din cadrul instituției care au nevoie de acces la date pentru a-și îndeplini atribuțiile.
   - **Exemple:**
     - Departamentul resurse umane (pentru datele angajaților).
     - Compartimentul financiar-contabil
     - Conducerea instituției (pentru corespondență oficială).
2. **Destinatari externi:**
   - Entități sau persoane din afara instituției către care datele sunt transmise conform obligațiilor legale sau altor scopuri legitime.
   - **Exemple:**
     - Autorități publice (ex.: Direcția de Sănătate Publică, ITM, ANAF).
     - Pacienți sau reprezentanții legali ai acestora (pentru solicitări sau reclamații).
     - Alte instituții/organizații (ex.: parteneri contractuali, furnizori).

Cum să completezi coloana „Categorie destinatari"

Pentru fiecare activitate de prelucrare, trebuie să menționezi dacă destinatarii sunt

interni, **externi**, sau ambele categorii. Detaliile trebuie să fie specifice.

Exemple de completare:

Activitatea de prelucrare	Categorie destinatari
Gestionarea corespondenței oficiale	Interni: Conducerea instituției; Externi: Alte instituții/autorități
Emiterea adeverințelor pentru angajați	Interni: Departamentul resurse umane; Externi: ANAF, bănci (la cererea angajatului)
Înregistrarea cererilor/reclamațiilor	Interni: Compartimentele responsabile; Externi: Petiționarul (persoana care a depus cererea/reclamația)
Arhivarea documentelor	Interni: Departamentul secretariat, arhivă
Răspunsuri către autorități sau cetățeni	Externi: Direcția de Sănătate Publică, ITM, persoana care solicită informațiile

Aspecte de reținut la completare:

1. **Clasificarea precisă:**
   - Identifică fiecare tip de destinatar care are acces sau primește datele în mod direct.
2. **Transparența:**
   - Dacă datele sunt împărtășite cu destinatari externi, asigurați-vă că acest lucru este justificat prin temeiuri legale și menționat în notificările privind protecția datelor.
3. **Exemplu concret:**
   - Pentru cereri de adeverințe de salariu:**Intern:** Departamentul financiar-contabil.**Extern:** ANAF (pentru verificare fiscală) sau instituții bancare (la solicitarea angajatului).

XI.9. Coloana 9 - „Unde stocăm datele (arhiva fizică, pe server)"

În coloana **„Unde stocăm datele (arhiva fizică, pe server)"** trebuie să specificați exact locul și modul în care sunt stocate datele cu caracter personal prelucrate de secretariat. Este important să menționați dacă stocarea se face pe suport fizic (documente în arhive/dulapuri) sau în format electronic (servere, cloud, computere locale). Aceasta contribuie la evidențierea măsurilor de securitate luate pentru protejarea datelor.

Categorii posibile de stocare

1. **Arhivă fizică:**
   - Documentele pe suport hârtie (cereri, dosare, registre) sunt stocate în:
     - Dulapuri securizate.
     - Spații de arhivare dedicate și protejate.
2. **Servere locale:**
   - Fișierele electronice sunt stocate pe serverele interne ale instituției (protejate prin măsuri de securitate IT, cum ar fi acces controlat și back-up regulat).
3. **Cloud securizat:**
   - În unele cazuri, datele pot fi stocate în soluții cloud, dar numai dacă există asigurări de securitate și conformitate GDPR (de exemplu, furnizori certificați).
4. **Computere sau dispozitive locale:**
   - Documentele temporare sau fișierele sunt stocate pe computerele utilizate în secretariat, dar acestea trebuie să fie protejate prin parole și acces restricționat.

Exemple de completare a coloanei

Activitatea de prelucrare	Unde stocăm datele
Gestionarea corespondenței oficiale	Arhiva fizică (dulapuri securizate); Server intern
Emiterea adeverințelor pentru angajați	Arhiva fizică (dosare personale); Server intern
Înregistrarea cererilor/reclamațiilor	Arhiva fizică (registre); Server intern
Arhivarea documentelor	Arhiva fizică; Server dedicat arhivării electronice
Răspunsuri către autorități sau cetățeni	Server intern (fișiere electronice); Arhiva fizică

Cum să completezi corect:

1. **Pentru documentele fizice:**
   - Specifică unde sunt stocate documentele (ex.: dulapuri închise, spații de arhivă protejate).
2. **Pentru documentele electronice:**
   - Menționează platforma pe care sunt stocate:
     - „Server intern protejat" pentru fișierele din rețeaua instituției.
     - „Computere locale protejate" pentru fișiere stocate temporar.
     - „Cloud securizat" dacă instituția utilizează astfel de soluții.
3. **Combinații:**
   - Pentru procese care implică ambele formate (ex.: cereri redactate electronic, dar arhivate fizic), trece ambele locații.

Exemple detaliate pentru activități specifice:

- **Emiterea adeverințelor:**

- Documentul se redactează pe un computer și se stochează temporar pe serverul intern. După tipărire și semnare, adeverința este arhivată în format fizic în dosarul personal al angajatului.
- **Completare:** *„Server intern, arhivă fizică (dosar personal).”*

- **Gestionarea corespondenței oficiale:**
  - Corespondența primită se arhivează fizic, iar cea trimisă electronic este stocată pe servere.
  - **Completare:** *„Arhivă fizică (dulap securizat), server intern (e-mailuri).”*
- **Arhivarea documentelor:**
  - Documentele vechi se transferă în arhivă fizică, iar cele recente sunt păstrate pe servere.
  - **Completare:** *„Arhivă fizică, server dedicat arhivării electronice.”*

XI.10. Coloanele 10-11

Retentie/Cât timp se păstrează/Cadru legal

În coloana **„Retenție”**, trebuie să specificați perioada de timp pentru care datele cu caracter personal sunt păstrate, conform obligațiilor legale, normelor interne sau necesităților organizaționale. În coloana **„Cadru legal”**, trebuie să justificați durata de retenție prin menționarea actelor normative relevante (legi, regulamente, standarde interne).

Cum stabilești perioada de retenție:

1. **Conform legislației aplicabile:**
   - Unele documente au termene de păstrare prevăzute expres în legislație. De exemplu:
     - **Arhivarea documentelor:** Legea Arhivelor Naționale nr. 16/1996.
     - **Documente financiar-contabile:** Legea Contabilității nr. 82/1991.
2. **Conform normelor GDPR:**

- Art. 5 alin. (1) lit. e) din Regulamentul GDPR stipulează că datele trebuie păstrate doar pe perioada necesară scopului pentru care sunt prelucrate. După încheierea scopului, datele trebuie șterse sau anonimizate.

3. **În funcție de necesitățile operaționale:**
   - Pentru date fără un termen legal specific, instituția stabilește perioadele de păstrare prin politici interne.

Exemple de completare pentru compartimentul secretariat;

Tipul de date/documente	Perioadă de retenție	Cadru legal
Cereri/reclamații	5 ani	Legea nr. 16/1996 privind Arhivele Naționale.
Corespondența oficială	5 ani	Legea nr. 16/1996 privind Arhivele Naționale.
Documente financiar-contabile	10 ani	Legea Contabilității nr. 82/1991, art. 25.
Dosarele personale ale angajaților	75 ani (de la încetarea raportului de muncă)	Legea nr. 16/1996, HG 905/2017 privind registrul general de evidență a salariaților.
Înregistrările video (supraveghere)	Maximum 30 zile (sau mai puțin, conform scopului)	Art. 5 alin. (1) lit. e) GDPR.
Date despre programările la audiențe	1 an de la încheierea scopului	Politica internă; Art. 5 alin. (1) lit. e) GDPR.
Adeverințe eliberate pentru angajați	3 ani	Politica internă, în lipsa unei prevederi legale.

Ghid pentru completare:

1. Corespondență oficială

- **Retenție:** 5 ani.
- **Cadru legal:** Legea Arhivelor Naționale nr. 16/1996.

2. Cereri și reclamații ale cetățenilor

- **Retenție:** 5 ani după soluționare.
- **Cadru legal:** Legea nr. 16/1996.

3. Documente financiar-contabile (ex.: facturi, chitanțe, ordine de plată)

- **Retenție:** 10 ani.
- **Cadru legal:** Legea Contabilității nr. 82/1991, art. 25.

4. Dosare personale ale angajaților

- **Retenție:** 75 ani de la încetarea raportului de muncă.
- **Cadru legal:** Legea nr. 16/1996, HG 905/2017.

5. Înregistrări video (supraveghere CCTV)

- **Retenție:** Maximum 30 zile (sau mai puțin, conform scopului).
- **Cadru legal:** Art. 5 alin. (1) lit. e) GDPR.

6. Adeverințe eliberate pentru angajați

- **Retenție:** 3 ani de la emitere.
- **Cadru legal:** Politică internă a instituției, în lipsa unei prevederi legale specifice.

7. Programări la audiențe

- **Retenție:** 1 an de la finalizarea scopului.
- **Cadru legal:** Politica internă; Art. 5 alin. (1) lit. e) GDPR.

Recomandări pentru completare:

1. **Fii precis:** Include atât termenul de retenție, cât și sursa legală.
2. **Evidențiază diferențele:** Unele date sunt păstrate mai mult timp (ex.: dosare personale), în timp ce altele au un termen scurt (ex.: înregistrări video).
3. **Armonizare cu politica internă:** Dacă instituția are politici interne privind retenția datelor, acestea trebuie menționate.

XI.11 Coloanele 12-13
Cine intră în contact cu datele personale;

Cine are acces la datele cu caracter personal, specificând dacă este vorba despre angajați din cadrul instituției (personal intern) sau despre terțe părți care furnizează servicii externe (personal externalizat).

Această coloană ajută la identificarea persoanelor sau entităților care pot prelucra datele personale și asigură transparența asupra accesului la informațiile sensibile.

1. **Personal intern:**
    - Aceasta se referă la angajații instituției sau la persoanele care fac parte din structura internă a organizației și care au acces la datele prelucrate în îndeplinirea atribuțiilor lor.
    - **Exemple:**
        - Angajați ai secretariatului.

- Personal din departamentele administrative, financiar-contabile, resurse umane, achizitii, tehnic, medical, statistic si informaticaă etc.
- Conducerea instituției

2. **Personal externalizat**
   - Se referă la furnizori de servicii externe care prelucrează datele în numele instituției sau care au acces la date pentru îndeplinirea unui contract/obligație.
     - **Exemple:**
       - Companii externe de arhivare.
       - Furnizori de servicii IT sau de suport tehnic care gestionează serverele și datele electronice.
       - Firme de consultanță externă care se ocupă de achiziții, proiecte, etc.
       - Firmă de curățenie, de pază care au acces temporar la birouri, unde se află documente cu date personale.

Exemplu de completare a coloanei „Cine intră în contact cu datele?"

Activitatea de prelucrare	Cine intră în contact cu datele? Personal intern/Personal externalizat
Gestionarea corespondenței oficiale	Personal intern: Angajați ai secretariatului; Personal externalizat: Firma de curierat
Emiterea adeverințelor pentru angajați	Personal intern: Departament resurse umane; Personal externalizat: Contabil extern
Înregistrarea cererilor/reclamațiilor	Personal intern: Angajați secretariat; Personal externalizat: Firma de consultanță pentru soluționare reclamații
Arhivarea documentelor	Personal intern: Departament arhivă; Personal externalizat: Firmă de arhivare

Activitatea de prelucrare	Cine intră în contact cu datele? Personal intern/Personal externalizat
Supravegherea video (CCTV)	Personal intern: Responsabil IT, securitate; Personal externalizat: Furnizor de servicii IT (dacă există suport extern pentru mentenanță)
Gestionarea bazelor de date electronice	Personal intern: Departament IT, secretariat; Personal externalizat: Furnizor extern de suport IT

Cum să completați corect:

1. **Personal intern:**
   - Menționați departamentele sau funcțiile interne care au acces la date. De exemplu:
     - „Personal intern: Departament secretariat, departament IT, resurse umane."
2. **Personal externalizat:**
   - Specificați serviciile externe care au acces la date, în baza unui contract sau acord. De exemplu:

- „Personal externalizat: Firma de arhivare, furnizor IT pentru întreținerea serverelor."
- „Personal externalizat: Firmă consultanță în achiziții în vederea derulării unei anomie procedure sau proiect.

3. **Confidențialitate și securitate:**
   - Dacă există un furnizor extern care are acces la datele sensibile, asigurați-vă că există un acord de prelucrare a datelor semnat (DPA - Data Processing Agreement), care reglementează condițiile în care aceste date sunt accesate și procesate.

XI.12. Coloana 14; Relațiile între instituție și terți

În această coloană se înregistrează tipurile de rapoarte existente – trebuie descrisă natura relației contractuale sau profesională între instituție, S.A.J Iași și entitatea externalizată (societatea), precum și tipurile de documente, raportări sau obligații de informare care sunt parte din această relație.

Această coloană este importantă pentru a specifica cadrul legal în care are loc prelucrarea datelor, raportările și responsabilitățile fiecărei părți, pentru a asigura transparența și respectarea regulamentului GDPR.

Astfel, această coloană va ajuta la clarificarea tipurilor de relații și a responsabilităților în ceea ce privește prelucrarea datelor cu caracter personal între diferite entități implicate.

Tipuri de relații și ce trebuie completat:

1. **Operator - Persoană împuternicită (Procesator)**
    - **Definiție:** Operatorul este entitatea care stabilește scopul și mijloacele prelucrării datelor (de exemplu, SAJ). Persoana împuternicită (procesatorul) prelucrează datele în numele operatorului, conform instrucțiunilor acestuia (ex.: un furnizor de servicii IT care stochează sau prelucrează datele pe serverele sale).
    - **Ce trebuie completat:**
        - În această coloană se va preciza că SAJ este **Operator** și compania/societatea respectivă este **Persoană împuternicită** (Procesator).
        - Exemplu: „SAJ este Operator, [Numele Societății] este Procesator de date pentru prestarea serviciilor IT."
2. **Operatori asociați**
    - **Definiție:** Aceasta este o situație în care două sau mai multe entități (operatori) decid împreună scopurile și mijloacele prelucrării datelor. Fiecare operator are responsabilități clare în cadrul procesului de prelucrare a datelor.

- **Ce trebuie completat:**
  - Dacă există o relație între SAJ și altă entitate în care ambele entități sunt responsabile pentru prelucrarea datelor și stabilesc împreună scopurile și mijloacele prelucrării, se va menționa că ambele entități sunt **Operatori asociați.**
  - Exemplu: „SAJ și [Numele Societății] sunt Operatorii asociați pentru procesarea datelor pacientului în cadrul serviciilor de ambulanță."

3. **Operator - Persoană împuternicită / Operator - Persoană împuternicită**
   - **Definiție:** Acesta este un tip de relație în care există atât un operator care prelucrează datele, cât și una sau mai multe persoane împuternicite care prelucrează datele în numele operatorului, dar și persoane împuternicite care prelucrează date în numele altui operator (dacă sunt implicate mai multe entități).
   - **Ce trebuie completat:**
     - Se va preciza tipul exact de relație, în care există un **Operator** și mai multe entități care pot fi **Persoane împuternicite**.
     - Exemplu: „SAJ este Operator, iar [Numele Societății] este Persoană împuternicită pentru gestionarea datelor medicale ale pacienților. [Altă societate] este Persoană împuternicită pentru prelucrarea datelor financiare."

Ce trebuie completat în această coloană:

1. **Tipurile de rapoarte și relații legale între entitate și societate:**
   - În această coloană, vei specifica tipul raportului contractual sau serviciul externalizat și ce documente sau rapoarte sunt generate în cadrul acestei relații.
2. **Exemple de tipuri de relație și raportări:**
   - **Contract de prestări servicii IT (pentru întreținerea serverelor sau managementul bazelor de date):**
     - **Relație:** Contract de prestări servicii.

- **Tipuri de rapoarte:** Raport de activitate periodică (ex.: întreținerea și actualizarea sistemelor, backup, gestionarea securității IT).

- **Servicii de arhivare externalizate:**
  - **Relație:** Contract de arhivare și păstrare a documentelor.
  - **Tipuri de rapoarte:** Raport anual de audit al arhivării, raport de livrare sau retragere documente din arhivă.
- **Furnizor de servicii de curierat:**
  - **Relație:** Contract de furnizare servicii de livrare.
  - **Tipuri de rapoarte:** Raport de livrare/primire documente.
- **Consultanță privind serviciul de achizitie**
  - **Relație:** Contract de prestări servicii.
- **Tipuri de rapoarte:** Raport periodic
- **Servicii de supraveghere video (CCTV):**
  - **Relație:** Contract de servicii de monitorizare și întreținere CCTV.
  - **Tipuri de rapoarte:** Raport de mentenanță periodică, raport de incident (dacă este cazul).
- **Consultanță juridică externă:**
  - **Relație:** Contract de consultanță juridică.
  - **Tipuri de rapoarte:** Raport de conformitate legală, recomandări pentru protecția datelor.

Exemplu de completare a coloanei „Relație între SAJ IASI(entitate) și respectiva societate/colaborator"

Activitatea de prelucrare	Relație între noi (entitate) și respectiva societate
Gestionarea bazelor de date electronice	Contract de prestări servicii IT. Tipuri de rapoarte: Raport de întreținere IT, raport de securitate IT.
Supravegherea video	Contract de prestări servicii de monitorizare video. Tipuri de

Activitatea de prelucrare	Relație între noi (entitate) și respectiva societate
(CCTV)	rapoarte: Raport lunar de întreținere, raport de incident.
Arhivarea documentelor	Contract de arhivare externalizată. Tipuri de rapoarte: Raport de arhivare, raport de retragere documente.
Servicii de curierat	Contract de furnizare servicii de livrare. Tipuri de rapoarte: Raport de livrare/primire documente.
Consultanță juridică	Contract de consultanță juridică. Tipuri de rapoarte: Raport de conformitate GDPR, rapoarte legale periodice.

Cum să completați corect:

1. **Clarificați tipul relației:**
   - Este important să specificați ce tip de contract există între instituție și entitate (de exemplu: contract de prestări servicii, contract de consultanță, contract de furnizare produse/servicii).
2. **Enumerați rapoartele relevante:**
   - Indică documentele sau rapoartele care sunt generate periodic sau în funcție de nevoi, care sunt legate de prelucrarea datelor. Acestea pot include rapoarte financiare, rapoarte de activitate, rapoarte de securitate sau conformitate.
3. **Specificați periodicitatea:**
   - Dacă raportările sunt periodice, este util să menționezi frecvența (ex.: raport lunar, anual, trimestrial etc.).
4. **Asigurați transparența:**
   - Detaliile specifice despre aceste relații ajută la asigurarea transparenței în privința modului în care datele sunt prelucrate și gestionate de către terți.

XI.13.Coloana 15 - Risc

În coloana **„Risc"** din registrul de evidență a prelucrărilor de date cu caracter personal, trebuie să precizați posibilele riscuri la care sunt expuse datele cu caracter personal în urma prelucrării acestora. Riscurile pot include, dar nu se limitează la, accesul neautorizat, pierderea datelor, furtul acestora, modificarea sau distrugerea accidentală a datelor, precum și alte incidente care ar putea afecta drepturile și libertățile persoanelor vizate.

Ce trebuie completat în coloana „Risc"?

1. **Identificarea riscurilor:**
   - În această coloană, trebuie să precizați care sunt riscurile principale la care datele ar putea fi expuse în cadrul activităților de prelucrare.
   - Aceste riscuri pot include riscuri legate de securitatea datelor, precum accesul neautorizat, pierderea datelor sau manipularea acestora într-un mod care să încalce regulamentul GDPR.
2. **Exemple de riscuri:**
   - **Acces neautorizat:** Persoane neautorizate pot avea acces la datele personale (de exemplu, prin atacuri cibernetice, acces fizic necontrolat la locațiile unde sunt stocate datele).
   - **Furtul de date:** Datele cu caracter personal pot fi furate (de exemplu, prin hackere sau furt de dispozitive).
   - **Modificarea sau ștergerea accidentală a datelor:** Datele pot fi modificate sau șterse din greșeală de către personalul autorizat sau de către terți.
   - **Pierdere de date:** Datele pot fi pierdute din cauza unei erori tehnice sau a unei defecțiuni ale sistemului.
   - **Confidențialitate compromisă:** Datele ar putea fi divulgate în mod neautorizat, afectând confidențialitatea persoanelor vizate.

- **Nerespectarea termenelor legale de păstrare a datelor:** Datele ar putea fi păstrate mai mult decât este permis de lege, punând în pericol drepturile persoanelor vizate.

Exemplu de completare a coloanei „Riscul"

Tipul de activitate	Riscuri identificate
Prelucrarea datelor de identificare a pacientului	Acces neautorizat la bazele de date, pierderea datelor pacientului, furtul informațiilor sensibile.
Gestionarea documentelor de arhivă	Distrugerea accidentală a documentelor, acces neautorizat la arhive fizice.
Supravegherea video (CCTV)	Acces neautorizat la înregistrările video, divulgarea neautorizată a imaginii persoanelor filmate.
Transmiterea datelor prin email sau alte canale	Interceptarea datelor în timpul transmiterii, acces neautorizat la emailurile cu informații sensibile.
Prelucrarea datelor angajaților (fișe de salarii)	Furtul sau divulgarea salariilor și altor date sensibile, acces neautorizat la datele salariale.
Prestarea de servicii externe (IT, arhivare etc.)	Acces necontrolat la datele cu caracter personal de către furnizorii externi, riscuri legate de securitatea furnizorilor IT.

Cum să completați corect:

1. **Identificați riscurile semnificative:**
   - Evaluarea riscurilor trebuie să fie realistă și bazată pe activitățile specifice de prelucrare a datelor. Identifică cele mai probabile riscuri și asigură-te că sunt clar descrise.
2. **Fiți detaliați:**

- Încearcă să identifici fiecare risc potențial care poate apărea pe parcursul prelucrării datelor, având în vedere tipul de activitate (ex.: acces la date sensibile, pierdere de date, etc.).

3. **Clasificați riscurile:**
   - Dacă este posibil, puteți adăuga o descriere a gravității riscurilor (ex.: „risc înalt", „risc mediu" etc.), deși acest lucru se face de obicei în etapele de evaluare a impactului asupra protecției datelor (DPIA - Data Protection Impact Assessment).

Recomandări:

- **Evaluarea riscurilor** este un proces continuu și trebuie să fie revizuit periodic, mai ales atunci când apar modificări semnificative în activitatea de prelucrare a datelor sau în cadrul legal.
- **Măsurile de securitate** și **controlul accesului** sunt esențiale pentru a reduce aceste riscuri, iar înregistrarea acestora ajută la demonstrarea conformității cu cerințele GDPR.

XI.14. Coloana 16 „Persoana responsabilă la nivel de departament"

În coloana **„Persoana responsabilă la nivel de departament"** din registrul de evidență a prelucrării datelor cu caracter personal, trebuie să fie specificată persoana (sau persoanele) care sunt responsabile de gestionarea și protejarea datelor cu caracter personal în cadrul departamentului respectiv. Aceste persoane au atribuții clare în ceea ce privește respectarea reglementărilor GDPR și asigurarea unui control adecvat al prelucrării datelor.

Ce trebuie completat în această coloană:

1. **Numele persoanei responsabile:**
   - Se va menționa numele persoanei care este direct responsabilă pentru gestionarea și protecția datelor cu caracter personal în cadrul activităților de prelucrare din departamentul respectiv. De exemplu, poate fi un responsabil IT, un responsabil al

secretariatului, sau chiar un angajat care se ocupă de datele angajaților, pacienților sau colaboratorilor.

2. **Exemplu de completare:**

Activitatea de prelucrare	**Persoana responsabilă la nivel de departament**
Prelucrarea datelor angajaților	xxx - Responsabil Resurse Umane
Gestionarea bazelor de date electronice	xxx - Administrator IT
Supravegherea video (CCTV)	xxx- Responsabil Securitate
Arhivarea documentelor	xxx - Responsabil Arhivă
Prelucrarea cererilor/reclamațiilor	xxx - Secretar
Consultanță juridică	xxx - Jursit

3. **Funcția sau rolul persoanei:**
   - Este important să se specifice și funcția sau rolul acestei persoane, pentru a înțelege mai bine atribuțiile sale legate de protecția datelor. De exemplu: „Responsabil IT", „Coordonator Secretariat", „Responsabil Resurse Umane" etc.

Cum să completați corect:

1. **Atribuți persoana responsabilă:**
   - Asigurați-vă că persoana responsabilă este desemnată corect și că aceasta are autoritatea necesară pentru a implementa măsurile corespunzătoare de protecție a datelor.
2. **Funcția specifică:**
   - Este recomandat să includeți atât numele complet al persoanei, cât și funcția/rolul acesteia în cadrul departamentului pentru a clarifica responsabilitățile specifice legate de protecția datelor.
3. **Revederea periodică:**
   - Este important ca aceste informații să fie actualizate periodic, pentru a reflecta schimbările de personal sau de responsabilități.
4. **Accesul la date:**

- Persoanele responsabile vor trebui să aibă un acces adecvat la date și să fie instruite pentru a se conforma cerințelor GDPR și pentru a implementa măsuri de protecție a datelor, acolo unde este cazul.

Exemplu completat într-o situație practică:

Dacă un departament al Serviciului de Ambulanță Județean Iași (Ex.Compartimentul Statistică) prelucrează datele pacienților conform fiselor de solicitări, persoana responsabilă ar putea fi un angajat care are autoritatea de a gestiona aceste activități și de a se asigura că sunt respectate toate reglementările de protecție a datelor:

Activitatea de prelucrare	Persoana responsabilă la nivel de departament
Prelucrarea datelor pacienților conform fiselor de solicitare	Xxx – Statistician

Pentru desemnarea responsabililor privind prelucrarea datelor cu caracter personal, este recomandat să se emită o **decizie** sau o **dispoziție internă**. Această decizie va clarifica în mod formal atribuțiile și responsabilitățile persoanei respective în cadrul instituției sau departamentului, iar procesul va asigura transparență și conformitate cu reglementările GDPR.

Cum se procedează pentru desemnarea responsabililor:

1. **Emitere decizie internă / dispoziție oficială:**
   - Conducerea instituției (de exemplu, managerul) va emite o decizie sau o dispoziție în care sunt desemnați responsabilii pentru protecția datelor cu caracter personal.
   - Aceasta va include numele persoanelor desemnate, funcțiile acestora și responsabilitățile lor în conformitate cu regulamentul GDPR (de exemplu, gestionarea datelor, protecția acestora, monitorizarea conformității, etc.).

2. **Conținutul deciziei:**
    - **Desemnarea responsabilului:** Va fi indicat numele complet al persoanei desemnate ca responsabil pentru prelucrarea datelor.
    - **Funcția/rolul:** Funcția specifică a persoanei desemnate va fi menționată clar (ex. Responsabil IT, Responsabil Secretariat, Responsabil Resurse Umane).
    - **Atribuțiile specifice:** Se vor specifica atribuțiile legate de protecția datelor, inclusiv gestionarea documentelor, securitatea datelor, asigurarea respectării procedurilor interne și a reglementărilor GDPR.
    - **Durata mandatului:** În unele cazuri, mandatul responsabilului poate fi limitat pe o perioadă de timp, în funcție de politică internă (de exemplu, 1 an sau 2 ani).
    - **Semnătura și data:** Decizia trebuie semnată de către persoana autorității competente (de obicei, conducerea instituției) și datată.

Pași suplimentari:

- **Informarea angajaților:** După emiterea deciziei, este esențial ca persoanele desemnate să fie informate oficial și să primească instrucțiuni clare privind responsabilitățile lor.
- **Instruirea și suportul continuu:** Persoanele desemnate trebuie să beneficieze de instruire continuă privind protecția datelor, reglementările GDPR și măsurile de securitate, pentru a putea îndeplini corect atribuțiile lor.
- **Revizuirea periodica:** Decizia ar trebui să fie revizuită periodic, mai ales dacă se fac modificări în structura organizațională sau în activitățile de prelucrare a datelor.

XI.15.Coloana 17 – Măsuri de securitate

În activitatea SAJ Iași, măsurile de securitate trebuie să fie foarte bine definite pentru a proteja datele cu caracter personal împotriva accesului neautorizat, pierderii, distrugerii sau prelucrării ilegale.

Măsurile de securitate sunt esențiale pentru protejarea datelor cu caracter personal împotriva accesului neautorizat, pierderii, distrugerii sau prelucrării ilegale. Aceste măsuri sunt împărțite în categorii tehnice, organizatorice și fizice. În această secțiune sunt prezentate măsurile care trebuie implementate pentru asigurarea unui nivel optim de securitate a datelor.

1. Măsuri tehnice

Aceste măsuri sunt legate de utilizarea tehnologiei pentru a proteja datele.

a. Protecția sistemelor informatice

- **Acces controlat la sistemele informatice:**
  - Utilizarea de parole complexe și unice pentru fiecare utilizator.
  - Limitarea accesului la bazele de date doar pentru personalul autorizat.
- **Sisteme de securitate IT:**
  - Implementarea unui firewall și a unui software antivirus actualizat constant.
  - Utilizarea criptării pentru transferul datelor sensibile (e.g., e-mailuri cu date personale).
- **Backup regulat:**
  - Salvarea periodică a datelor importante pe medii de stocare securizate.

- Stocarea copiilor de siguranță în locații protejate, separate de sistemele principale.

b. Monitorizarea activităților

- Utilizarea de loguri pentru a monitoriza accesul și modificările asupra fișierelor.
- Audituri periodice ale sistemelor informatice pentru a identifica și remedia vulnerabilitățile.
- **2. Măsuri organizatorice**

Aceste măsuri vizează procesele și regulile interne pentru protecția datelor.

a. Acces limitat la date

- Doar personalul din secretariat și alte departamente autorizate (ex. resurse umane, financiar) are acces la datele gestionate.
- Fiecare angajat are un nivel de acces corespunzător atribuțiilor sale (principiul „necesității cunoașterii").

b. Instruirea personalului

- Instruirea periodică a angajaților cu privire la:
  - Regulile de protecție a datelor conform GDPR.
  - Recunoașterea tentativelor de phishing sau alte atacuri cibernetice.

c. Politici și proceduri interne

- Implementarea unei politici interne privind prelucrarea datelor.
- Stabilirea procedurilor pentru:
  - Gestionarea cererilor de acces, modificare sau ștergere a datelor.
  - Răspunsul la incidente de securitate.

3. Măsuri fizice

Aceste măsuri protejează spațiul în care sunt gestionate datele.

a. Acces controlat la spațiile fizice

- **Securizarea biroului secretariatului:**
  - Închiderea biroului și a dulapurilor în afara orelor de lucru.
  - Restricționarea accesului fizic la spațiu doar pentru personalul autorizat.
- **Supraveghere video:**
  - Instalarea camerelor de supraveghere la intrarea în birou, cu respectarea legislației GDPR.

b. Protecția documentelor fizice

- **Stocarea documentelor în dulapuri securizate:**
  - Documentele sensibile (e.g., dosare administrative) trebuie păstrate în dulapuri încuiate.
- **Arhivarea corectă a documentelor:**
  - Documentele vechi sunt transferate în arhivă sau distruse conform politicii de retenție a datelor.

c. Eliminarea documentelor sensibile

- Distrugerea documentelor care nu mai sunt necesare folosind un distrugător de documente (nivel de securitate P-4 sau mai mare).

4.Măsuri tehnice suplimentare care trebuie implementate pentru asigurarea

unui nivel optim de securitate a datelor:

1.Autentificare Multi-Factor (MFA)

- **Descriere:**
  Autentificarea multi-factor (MFA) presupune utilizarea a două sau mai multe metode de autentificare pentru a accesa sistemele informatice. Aceste metode pot include parole complexe, coduri trimise prin SMS sau aplicații de autentificare.
- **Importanță:**
  MFA adaugă un strat suplimentar de protecție, asigurându-se că datele sunt accesate doar de persoane autorizate, chiar dacă parola este compromisă.
- **Implementare:**
  Toți angajații trebuie să activeze MFA pe conturile care au acces la datele cu caracter personal. Acest lucru se aplică sistemelor interne, e-mailurilor de serviciu și platformelor de gestionare a documentelor.

2. Controlul Accesului la Nivel de Aplicație

- **Descriere:**
  Aceasta măsură presupune configurarea unui sistem de permisiuni care limitează accesul utilizatorilor la datele sensibile, în funcție de rolul acestora.
- **Importanță:**
  Această practică garantează că numai persoanele care au nevoie de acces la date pentru îndeplinirea sarcinilor lor vor avea acest drept, reducând riscul de acces neautorizat.
- **Implementare:**
  În fiecare aplicație care manipulează datele personale, vor fi setate permisiuni de acces conform rolurilor și atribuțiilor fiecărui angajat. De exemplu, angajații care nu se ocupă direct cu gestionarea datelor pacienților nu vor avea acces la informațiile acestora.

3. Evaluarea și Testarea Periodică a Securității IT

- **Descriere:**
  Evaluarea periodică a securității IT include efectuarea de teste și audituri pentru identificarea vulnerabilităților și evaluarea eficienței măsurilor de protecție implementate.
- **Importanță:**
  Testele de securitate ajută la descoperirea și corectarea eventualelor puncte slabe, reducând riscul de exploatare a acestora de către atacatori.
- **Implementare:**
  SAJ va organiza periodic audituri de securitate și teste de penetrare (pentru a simula un atac cibernetic), pentru a identifica și corecta orice vulnerabilități în sistemele informatice.

4. Protecția Datelor în Tranzit și în Repaus

- **Descriere:**
  Protecția datelor în tranzit se referă la securizarea datelor în timpul transferului (ex.: prin e-mail sau rețele), iar protecția datelor în repaus se referă la securizarea acestora atunci când sunt stocate pe servere sau dispozitive de stocare.
- **Importanță:**
  Fără protecția adecvată a datelor, acestea pot fi interceptate în tranzit sau accesate în mod neautorizat în timpul stocării, ceea ce poate duce la scurgeri de informații sensibile.
- **Implementare:**
  - **Protecția datelor în tranzit:** Datele care conțin informații sensibile vor fi criptate folosind protocoale de securitate moderne (ex.: TLS pentru e-mailuri și HTTPS pentru accesul web).
  - **Protecția datelor în repaus:** Toate datele stocate pe servere vor fi criptate folosind soluții de criptare puternice, asigurându-se că datele rămân protejate chiar și în cazul unui atac fizic asupra serverelor.

5. Backup Regulamentar al Datelor

- **Descriere:**
  Backup-ul regulat implică salvarea periodică a datelor importante într-un loc sigur, pentru a asigura recuperarea acestora în caz de atac cibernetic sau defecțiune tehnică.
- **Importanță:**
  În cazul unui incident de securitate, backup-urile permit restaurarea rapidă a datelor și minimizarea impactului asupra activității.
- **Implementare:**
  SAJ va efectua backup-uri periodice ale datelor importante pe medii de stocare securizate. Copiile de siguranță vor fi stocate într-o locație separată și protejate împotriva accesului neautorizat.

6. Monitorizarea Activităților Utilizatorilor

- **Descriere:**
  Monitorizarea activităților presupune urmărirea și înregistrarea comportamentului utilizatorilor în sistemele informatice, pentru a detecta eventuale activități neautorizate.
- **Importanță:**
  Această măsură ajută la identificarea rapidă a accesului neautorizat sau a modificărilor nejustificate asupra datelor personale.
- **Implementare:**
  Toate sistemele care manipulează datele cu caracter personal vor fi configurate pentru a înregistra loguri de acces și modificări. Aceste loguri vor fi revizuite periodic pentru a detecta comportamente neautorizate.

Exemple de implementare a măsurilor de securitate

Măsură de securitate	Exemplu de aplicare concretă
Acces controlat la date	Fiecare angajat din secretariat folosește un cont individual pentru accesarea fișierelor informatice.
Backup al datelor	Datele corespondenței oficiale sunt salvate zilnic pe un server securizat.
Închiderea biroului	La finalul zilei, biroul secretariatului este încuiat, iar documentele sunt depozitate în dulapuri securizate.
Instruirea personalului	Angajații participă la un curs anual de protecție a datelor.
Supravegherea video	Intrarea în zona biroului este monitorizată prin camere de securitate cu respectarea GDPR.
Distrugerea documentelor	Actele expirate sunt distruse utilizând un distrugător certificat pentru documente confidențiale.

XII.Instrucțiuni, explicații și exemple de completare a Registrului de Prelucrare a Datelor cu Caracter Personal în cadrul serviciilor/compartimentelor/ birourilor.

În conformitate cu Regulamentul General privind Protecția Datelor (GDPR), Serviciul de Ambulanță Județean Iași (SAJ) are obligația de a documenta în mod detaliat activitățile de prelucrare a datelor cu caracter personal. Registrul de Evidență a Prelucrării Datelor cu Caracter Personal al SAJ este un instrument esențial pentru asigurarea transparenței și conformității cu

reglementările europene și naționale privind protecția datelor. Acesta facilitează monitorizarea și controlul activităților de prelucrare, contribuind la protejarea drepturilor persoanelor vizate și asigurarea unui management responsabil al datelor personale.

Registrul este structurat în 17 coloane, fiecare reflectând un aspect important al procesului de prelucrare a datelor. Completarea corectă a fiecărei coloane este esențială pentru asigurarea respectării principiilor GDPR, inclusiv transparența, legalitatea, exactitatea și minimizarea prelucrării datelor.

Capitolul „Instrucțiuni specifice de completare a registrului" din cadrul acestei proceduri operaționale oferă clarificări detaliate pentru fiecare coloană, având rolul de a ghida personalul responsabil în completarea corectă a registrului, conform cerințelor legale și interne. Prin urmare, este esențial ca fiecare coloană să fie completată cu informații precise și actualizate, pentru a asigura trasabilitatea și conformitatea proceselor de prelucrare a datelor personale.

Cele 17 coloane, descrise în detaliu în acest capitol, includ aspecte precum proveniența datelor, scopul prelucrării, temeiul legal, destinatarii datelor, măsurile de securitate și durata păstrării acestora. De asemenea, se vor preciza măsurile de protecție a datelor și persoanele responsabile la nivel de departament sau serviciu, pentru a asigura un control riguros asupra procesului de prelucrare.

Instrucțiunile specifice sunt destinate tuturor angajaților și persoanelor desemnate din cadrul SAJ care gestionează și prelucrează date personale, asigurând astfel un cadru coerent și transparent în activitățile de prelucrare a datelor cu caracter personal. Este esențial ca fiecare compartiment sau serviciu să cunoască responsabilitățile și obligațiile care îi revin în acest proces, pentru a proteja în mod eficient datele personale și pentru a respecta reglementările în vigoare.

XII.1. Rolul Instrucțiunilor cu explicații și exemple în Procedura Operațională

Instrucțiunile și exemplele structurate pe compartimente și servicii incluse în această procedură au rolul de a clarifica modul de completare a Registrului de Evidență a Datelor cu Caracter Personal în cadrul Serviciului de Ambulanță Județean Iași. Acestea sunt menite să ofere îndrumări practice pentru fiecare compartiment și serviciu în parte, astfel încât să asigure uniformitatea și corectitudinea în aplicarea normelor stabilite prin GDPR.

Rolul principal al exemplelor este de a:

- **Clarifica pașii specifici**: Exemplele ajută la înțelegerea exactă a informațiilor care trebuie completate în registru, eliminând ambiguitățile și asigurând o completare corectă a câmpurilor.
- **Asigura consistența**: Prin furnizarea unor modele concrete, exemplele garantează că toate compartimentele și serviciile urmează aceleași standarde în completarea documentației și în aplicarea procedurii.
- **Facilita instruirea și implementarea**: Exemplele contribuie la formarea personalului, explicând în mod practic cum să aplice procedura în activitățile zilnice, asigurând astfel o implementare eficientă a reglementărilor GDPR.
- **Oferi îndrumare pentru cazuri specifice**: Exemplele acoperă situații diverse, care pot apărea în diverse compartimente sau pentru diferite tipuri de date, oferind astfel un ghid aplicabil diverselor scenarii.

Este important ca exemplele să fie folosite ca referințe și să fie adaptate în funcție de specificul fiecărei activități sau compartiment, astfel încât să reflecte corect tipologia datelor prelucrate și relațiile de prelucrare între entitățile implicate.

XI.2. Compartimentul Resurse Umane;

1. Activitatea de Prelucrare

- **Exemplu activitate**: Prelucrarea datelor angajaților pentru gestionarea resurselor umane (angajare, concedii, evaluări de performanță, salarizare).
- **Detaliu**: Activitățile de prelucrare includ colectarea, stocarea și actualizarea datelor angajaților, gestionarea concediilor, monitorizarea performanței și a absenteismului, întocmirea fișelor de salarii și raportările către autoritățile competente.

2. Cadrul Legal

- **Articolul 6 alin. (1) lit. c** - „îndeplinirea unei obligații legale": Prelucrarea este necesară pentru respectarea obligațiilor legale privind raportările financiare, de muncă și fiscale.
- **Articolul 6 alin. (1) lit. b** - „executarea unui contract": Prelucrarea este necesară pentru executarea contractului de muncă (plăți salariale, evaluări de performanță).
- **Articolul 9 alin. (2) lit. b** - „prelucrarea datelor sensibile pentru monitorizarea stării de sănătate și efectuarea de evaluări periodice ale stării de sănătate ale angajaților".

3. Scopul Prelucrării

- **Exemple de scopuri**:
  - Gestionarea contractelor de muncă și a documentației aferente.
  - Calcularea și plata salariilor și a altor beneficii.
  - Gestionarea concediilor și absențelor.
  - Evaluarea performanței angajaților.
  - Respectarea obligațiilor legale (de exemplu, raportarea către autoritățile fiscale sau de muncă).
  - Organizarea și coordonarea programelor de formare continuă.

4. Tipuri de Date Colectate

- **Date personale**: Nume, prenume, CNP, adresă, număr de telefon, email.
- **Date profesionale**: Funcție, salariu, istoricul profesional, calificări, evaluări de performanță, concedii medicale și de odihnă.
- **Date sensibile** (dacă este cazul): Informații privind starea de sănătate (pentru concedii medicale, evaluări de sănătate pentru condiții de muncă specifice, etc.).

5. Destinatarii Datelor

- **Destinatari interni**:
  - Managerii de departamente pentru evaluarea performanței.
  - Contabilitatea/Departamentul financiar pentru procesarea salariilor.
  - Serviciul de resurse umane pentru gestionarea dosarelor angajaților.
- **Destinatari externi**:
  - Autoritățile fiscale și de muncă (ANAF, ITM) pentru raportările obligatorii.
  - Companii de asigurări pentru înregistrarea angajaților în cadrul asigurărilor de sănătate, pensii, etc.

6. Perioada de Păstrare a Datelor

- **Perioadă de păstrare**:
  - **Datele angajaților**: conform legislației naționale, datele vor fi păstrate pe întreaga durată a raporturilor de muncă și pentru o perioadă de 3 ani după încetarea acestora (pentru scopuri fiscale și de raportare).
  - **Datele sensibile**: Perioada de păstrare poate fi determinată de tipul documentului (ex: certificate medicale păstrate conform reglementărilor în vigoare).

7. Măsuri de Securitate

- **Măsuri tehnice**:

- Protecția datelor prin criptare.
- Sisteme de control al accesului la bazele de date.
- Utilizarea parolelor complexe pentru accesul la fișierele confidențiale.
-

- **Măsuri organizatorice**:
  - Accesul la datele angajaților este restricționat doar la personalul autorizat.
  - Formarea continuă a personalului în privința protecției datelor și a confidențialității.
  - Revizuirea periodică a procedurilor de securitate și implementarea de noi măsuri pe baza evaluării riscurilor.
  -

8. Persoane Responsabile la Nivel de Compartiment

- **Responsabil în cadrul Serviciului Resurse Umane**:
  - Persoana responsabilă pentru implementarea și monitorizarea respectării procedurilor de protecție a datelor cu caracter personal.
  - Exemple de roluri: Șef serviciu Resurse Umane, Responsabil protecția datelor (DPO) în cadrul serviciului.

9. Transferuri Internaționale de Date

- Dacă datele sunt transferate în afacerea Uniunii Europene sau în afacerea SEE, se menționează măsurile de protecție pentru respectarea prevederilor GDPR, precum utilizarea unor clauze contractuale standard sau alte mecanisme de transfer securizate.

10. Drepturile Persoanelor Vizate

- **Drepturi ale angajaților**:
  - Dreptul de acces la propriile date.
  - Dreptul de rectificare și ștergere a datelor.

- Dreptul de a solicita restricționarea prelucrării.
- Dreptul de a depune o plângere la autoritatea de supraveghere (ANSPDCP).

Cum se Completează Registrul pentru Serviciul Resurse Umane:

- **Activitatea de Prelucrare**: Detalierea fiecărei activități relevante (ex: colectarea și prelucrarea datelor angajaților pentru contractele de muncă).
- **Cadrul Legal**: Se vor completa articolele corespunzătoare din GDPR și legislația națională (ex: Art. 6 alin. (1) lit. c și Art. 9 alin. (2) lit. b).
- **Scopul Prelucrării**: Explicarea scopurilor clare ale prelucrării datelor (ex: administrarea dosarului de angajare, evaluarea performanței, raportări fiscale).
- **Tipurile de Date Colectate**: Specificarea datelor personale și sensibile care sunt colectate de serviciul de resurse umane.
- **Destinatarii Datelor**: Precizarea persoanelor interne (ex: departamente) și externe (ex: autorități) care pot accesa datele.
- **Perioada de Păstrare a Datelor**: Stabilirea perioadei de păstrare conform reglementărilor legale.
- **Măsuri de Securitate**: Detalierea măsurilor implementate pentru protejarea datelor.
- **Persoane Responsabile**: Nominalizarea persoanelor responsabile de protecția datelor în cadrul serviciului de resurse umane.

Exemple detaliate din cadrul compartimentului **Resurse Umane**, care ilustrează activitățile de prelucrare a datelor cu caracter personal și care ar trebui incluse în registrul de evidență a prelucrării datelor cu caracter personal, adaptat la GDPR.

1. Gestionarea Contractelor de Muncă

Activitate: Colectarea și gestionarea documentelor necesare pentru încheierea și administrarea contractelor de muncă (ex: CV, copii ale actelor de identitate, acte de studii, fișe de angajare).

- **Tipuri de date colectate**:
  - Date de identificare (nume, prenume, CNP, dată naștere, adresă).
  - Date de contact (telefon, e-mail).
  - Date profesionale (experiență profesională, calificări, studii).
- **Scopul prelucrării**:
  - Îndeplinirea obligației legale de încheiere și gestionare a contractelor de muncă.
  - Crearea unui dosar personal de angajare.
- **Temeiul legal**:
  - Articolul 6 alin. (1) lit. b) „executarea unui contract".
  - Articolul 6 alin. (1) lit. c) „îndeplinirea unei obligații legale" (ex: raportări fiscale).
- **Destinatari**:
  - Managerul General al S.A.J IASI, sindcat in vederea acordului si pentru aprobarea angajării.
  - Autoritățile fiscale pentru raportările obligatorii (ANAF, ITM, DSP, Ministerul Sanatații, etc).
- **Măsuri de securitate**:
  - Stocarea documentelor într-un sistem informatic securizat cu acces restricționat.
  - Protejarea dosarelor fizice (închise în arhive accesibile doar persoanelor autorizate).

2. Plata Salariilor și Beneficiilor

Activitate: Colectarea datelor necesare pentru calcularea și plata salariilor și beneficiilor angajaților (ex: ore lucrate, sporuri, taxe și impozite, deduceri, bonusuri).

- **Tipuri de date colectate**:
  - Date financiare (salariu, deduceri, bonusuri).
  - Date de identificare (nume, prenume, CNP).
  - Date bancare (IBAN).

- **Scopul prelucrării**:
  - Asigurarea plății corecte și în timp util a salariilor.
  - Calcularea impozitelor și contribuțiilor.
- **Temeiul legal**:
  - Articolul 6 alin. (1) lit. c) „îndeplinirea unei obligații legale" (raportările fiscale, calcularea taxelor).
  - Articolul 6 alin. (1) lit. b) „executarea unui contract" (plata salariilor conform contractului de muncă).
- **Destinatari**:
  - Departamente interne: contabilitate, management financiar.
  - Instituții externe: ANAF, case de pensii, bănci.
- **Măsuri de securitate**:
  - Criptarea fișierelor financiare.
  - Acces controlat la datele salariale.
  - Backup regulat pentru prevenirea pierderii de date.

3. Gestionarea Concediilor și Absențelor

Activitate: Înregistrarea și gestionarea cererilor de concediu (vacanță, medical, de odihnă) și a absențelor angajaților.

- **Tipuri de date colectate**:
  - Date de identificare (nume, prenume, CNP).
  - Tipul și durata concediului (de odihnă, medical, alte absențe).
  - Date referitoare la starea de sănătate (în cazul concediilor medicale).
- **Scopul prelucrării**:
  - Gestionarea corectă a timpului liber acordat angajaților.
  - Asigurarea respectării normelor legale privind drepturile de concediu.
- **Temeiul legal**:

- Articolul 6 alin. (1) lit. c) „îndeplinirea unei obligații legale" (ex: respectarea reglementărilor privind concediile de odihnă, medicale).
- Articolul 9 alin. (2) lit. h) „prelucrarea datelor sensibile pentru tratamente medicale" (în cazul concediilor medicale).

- **Destinatari**:
  - Manageri de departamente (pentru aprobare concedii).
  - Autorități externe (ex: instituțiile de asigurări sociale pentru concediile medicale).
- **Măsuri de securitate**:
  - Depozitarea dosarelor de concedii în sisteme de gestionare a documentelor protejate.
  - Acces restricționat la datele sensibile (ex: certificate medicale).

4. Evaluarea Performanței Angajaților

Activitate: Prelucrarea datelor referitoare la evaluările de performanță ale angajaților (ex: evaluări anuale, feedback-ul managerilor, obiectivele îndeplinite).

- **Tipuri de date colectate**:
  - Date profesionale (performanță, realizări, calificative).
  - Date de feedback (comentarii manageriale).
- **Scopul prelucrării**:
  - Evaluarea competențelor și performanței angajaților.
  - Dezvoltarea profesională și implementarea de măsuri pentru îmbunătățirea performanței.
- **Temeiul legal**:
  - Articolul 6 alin. (1) lit. b) „executarea unui contract" (ex: evaluări pentru dezvoltarea carierei).
  - Articolul 6 alin. (1) lit. f) „interesul legitim al angajatorului" (în scopuri de management al resurselor umane și performanță).

- **Destinatari**:
  - Managerii de departamente pentru implementarea măsurilor de îmbunătățire a performanței.
  - Angajații (pentru informarea privind evaluările).
- **Măsuri de securitate**:
  - Protecția fișierelor cu evaluări prin criptare.
  - Acces controlat pe bază de roluri pentru manageri și HR.

5. Formarea Profesională și Dezvoltarea Angajaților

Activitate: Gestionarea programelor de formare continuă pentru angajați (ex: cursuri, certificări, sesiuni de training).

- **Tipuri de date colectate**:
  - Date de identificare (nume, prenume).
  - Date privind cursurile urmate (tipul cursului, data finalizării, certificări obținute).
- **Scopul prelucrării**:
  - Planificarea și urmărirea dezvoltării profesionale a angajaților.
  - Îmbunătățirea competențelor necesare pentru îndeplinirea rolurilor de muncă.
- **Temeiul legal**:
  - Articolul 6 alin. (1) lit. b) „executarea unui contract" (pentru a respecta cerințele de formare profesională).
  - Articolul 6 alin. (1) lit. f) „interesul legitim al angajatorului" (pentru îmbunătățirea competențelor angajaților).
- **Destinatari**:
  - Managerii de departamente pentru identificarea nevoilor de formare.
  - Firmele de training externe pentru livrarea cursurilor.
- **Măsuri de securitate**:
  - Păstrarea documentației privind formarea în sisteme protejate.

- Acces limitat la datele despre formare, numai pentru personalul HR și Managerul Instituției.

6. Concursurile pentru angajare

In cadrul concursurilor pentru anagajare, **datele cu caracter personal** colectate de către compartimentul Resurse Umane sunt esențiale pentru evaluarea candidaților și selecția acestora. Aceste date trebuie gestionate cu respectarea strictă a reglementărilor GDPR. Iată câteva exemple de date cu caracter personal care ar putea fi colectate:

1. Date de Identificare

- **Nume și prenume**
- **Data nașterii**
- **CNP** (Cod Numeric Personal)
- **Adresă**
- **Număr de telefon**
- **Adresă de email**
- **Sex** (în unele cazuri)

2. Date Educaționale

- **Studii și calificări** (ex: diplomă de bacalaureat, licență, masterat, cursuri de specializare, etc.)
- **Instituțiile de învățământ absolvite**
- **Date privind performanțele academice** (medii, premii etc.)

3. Experiență Profesională

- **Locuri de muncă anterioare** (nume angajator, funcția ocupată, perioadă de muncă)
- **Obiective și realizări profesionale**

4. Date privind Evaluarea Candidaturii

- **Scrisoare de intenție**
- **CV-ul** (care poate include informații suplimentare despre interesele personale și realizările candidatului)
- **Testele de competență** (rezultate la probele de concurs, note, evaluări)
- **Interviuri** (notația și evaluările făcute de comisia de selecție)

5. Date Sensibile (în anumite cazuri)

- **Starea de sănătate** (în cazul în care concursul presupune evaluarea aptitudinilor fizice sau alte condiții specifice de sănătate)
- **Date privind apartenența sindicală** (dacă este relevant pentru post)
- **Date privind apartenența etnică sau rasială** (dacă sunt necesare pentru respectarea reglementărilor de diversitate)

6. Date de Contact

- **Număr de telefon mobil și/sau fix**
- **Adresă de e-mail**

7. Date Referitoare la Participarea la Concurs

- **Data și ora la care candidatul se prezintă la concurs**
- **Locația concursului**
- **Rezultatele fiecărei etape a concursului** (probă scrisă, interviu, etc.)
- **Observații ale comisiei de selecție**

8. Alte Date Specifice

- **Preferințele de locație** (dacă candidatul are o preferință pentru un anumit loc de muncă)
- **Disponibilitatea de a începe lucrul**

- **Condiții speciale de muncă** (de exemplu, disponibilitatea de a lucra în ture, deplasări, etc.)

În cadrul acestui proces, toate aceste date sunt colectate pentru a evalua competențele, experiența și eligibilitatea candidaților în raport cu cerințele postului disponibil. Este important ca toți acești pași să fie documentați corect în conformitate cu **Regulamentul (UE) 679/2016 (GDPR)** și să fie menționat temeiul legal pentru fiecare prelucrare a datelor (de exemplu, **Articolul 6(1)(b)** - executarea unui contract, **Articolul 9(2)(b)** - procesul de recrutare în scopul de a îndeplini obligațiile legale ale angajatorului).

In contextul celor prezentate, Registrul de prelucrare a datelor cu caracter personal este un instrument esențial pentru orice organizație, în special pentru un serviciu de ambulanță, pentru toate departamentele, serviciile și compartimentele, pentru a asigura conformitatea cu reglementările **GDPR** (Regulamentul (UE) 679/2016). Acesta ajută la gestionarea și monitorizarea modului în care datele personale sunt colectate, stocate, prelucrate și partajate, protejând astfel drepturile persoanelor vizate și asigurând transparența în procesul de prelucrare.

XII.3. Compartimentul /Serviciul Achiziții;

În cadrul compartimentului **achiziții** al Serviciului de Ambulanță Iași, registrul de prelucrare a datelor cu caracter personal trebuie completat pentru a reflecta specificul activităților legate de procesul de achiziție.

Exemple de Prelucrare a Datelor în Compartimentul Achiziții din cadrul S.A.J. Iași

Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră î Contact cu Datele
Organizarea și derularea achizițiilor publice	Nume, CNP, date de contact (telefon, email), documente fiscale (CUI, CIF, cont	Reprezentanți ai furnizorilor, personal implicat în procesul de	Art. 6(1)(c) - obligație legală; Art. 6(1)(e) -	Documentele fizice păstrate în dulapuri securizate, acces electronic	5 ani de la finalizarea contractului (Legea 98/2016)	ANAF, autorități de audit, Curtea de Conturi	Arhiva fizică, server securizat al instituției	Personal din departament achiziții

Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră î Contact cu Datele
	bancar)	achiziții	interes public	limitat pe servere protejate				
Monitorizarea derulării contractelor	Nume, semnături, date de identificare ale reprezentanților contractanților	Furnizori, colaboratori	Art. 6(1)(c) - obligație legală	Sistem electronic de gestionare a documentelor criptat	10 ani (Codul fiscal, art. 25)	Curtea de Conturi, instanțe de judecată	Arhiva fizică, sistem de management al documentelor	Personal autorizat din achiziții

Explicații Detaliate pentru Fiecare Coloană

1. **Scopul Prelucrării**:
   - Exemplu: "Organizarea și derularea procedurilor de achiziții publice", "Monitorizarea și raportarea în cadrul derulării contractelor".
   - Se justifică în baza obligațiilor legale ale instituției.
2. **Tipul de Date Colectate**:
   - Date personale identificabile: nume, prenume, semnătură, date de contact.
   - Date financiare și fiscale: CUI, CIF, cont bancar, date din facturi sau contracte.
3. **Persoane Vizate**:
   - Reprezentanți legali ai furnizorilor, colaboratori implicați în derularea contractelor.
4. **Temei Legal**:
   - Art. 6(1)(c): Obligația legală de a derula achiziții publice conform **Legii 98/2016** privind achizițiile publice.
   - Art. 6(1)(e): Interes public justificat de asigurarea transparenței și controlului asupra fondurilor publice.
5. **Măsuri de Securitate**:
   - Fizice: Documente păstrate în dulapuri securizate cu acces restricționat.

- Tehnice: Stocarea documentelor pe servere securizate, acces electronic limitat pe bază de parole și roluri definite.
- Organizatorice: Personalul instruite în conformitate cu GDPR.

6. **Durata Păstrării**:
   - Conform legislației, documentele legate de achiziții trebuie păstrate:
     - **5 ani**: După finalizarea procedurii de achiziție, conform **Legii 98/2016**.
     - **10 ani**: Pentru documente cu relevanță fiscală, conform **Codului fiscal, art. 25.**
7. **Destinatari**:
   - Autorități de reglementare (ex. ANAF, Curtea de Conturi, autorități de audit).
   - Instanțe de judecată, în cazul litigiilor.
8. **Unde Stocăm Datele**:
   - Documentele fizice sunt păstrate în arhiva fizică a instituției.
   - Documentele electronice sunt stocate pe servere interne protejate, în sisteme de management al documentelor (ex. SEAP).
9. **Cine Intră în Contact cu Datele**:
   - Personalul din departamentul achiziții.
   - Alte departamente interne care gestionează bugetul, juridicul sau auditul.

Alte Exemple de Prelucrare a Datelor în Achiziții

1. **Publicarea în SEAP**:
   - Datele colectate pentru publicarea anunțurilor: informații despre ofertanți, date de contact, declarații de eligibilitate.
2. **Raportarea către Autorități**:
   - Date incluse în rapoartele către ANAP (Autoritatea Națională pentru Achiziții Publice): documentații, copii ale contractelor, situații financiare.
3. **Verificarea Eligibilității Ofertanților**:

- Date prelucrate: certificate de atestare fiscală, cazier judiciar, alte documente solicitate pentru conformitatea cu legislația.

XII.4. Compartimentul legislație – contencios;

Compartimentul juridic dintr-o instituție precum Serviciul de Ambulanță Iași gestionează date cu caracter personal legate de activitățile sale, cum ar fi reprezentarea în instanță, redactarea și gestionarea contractelor, soluționarea litigiilor, și consultanța juridică.

Importanța Registrului de Evidență a Prelucrării Datelor în Compartimentul Juridic

Registrul de evidență a prelucrării datelor cu caracter personal este esențial pentru compartimentul juridic al unui serviciu de ambulanță, deoarece documentează în mod transparent și complet modul în care datele sunt prelucrate în scopuri juridice. Importanța sa poate fi detaliată astfel:

1. Conformarea cu Regulamentul GDPR (UE) 679/2016

- **Obligație legală**: Articolul 30 din GDPR impune întocmirea și actualizarea unui registru care să descrie toate activitățile de prelucrare a datelor.
- **Evita sancțiunile**: Registrul este un instrument esențial pentru demonstrarea conformității în fața autorității de supraveghere (ANSPDCP) în cazul unui control.
- **Gestionarea riscurilor**: Ajută compartimentul juridic să identifice riscurile legate de confidențialitatea datelor și să implementeze măsuri adecvate pentru minimizarea acestora.

2. Protejarea Datelor Sensibile

În activitatea compartimentului juridic se prelucrează date personale și sensibile, precum:

- Date de identificare (nume, CNP, adresă).

- Informații privind litigiile (dosare, probe, sentințe).
- Date legate de contracte (reprezentanți legali, semnături).

Registrul detaliază măsurile de securitate fizice, tehnice și organizaționale luate pentru protecția acestor date, respectând principiile de **legalitate**, **echitate** și **transparență**.

3. Rol Strategic în Organizare

- **Managementul informațiilor**: Registrul permite o evidență clară a datelor procesate și oferă o bază pentru decizii informate în cazul litigiilor sau al controalelor.
- **Fluxuri de date bine definite**: Ajută la delimitarea clară a atribuțiilor și accesului la date în cadrul echipei juridice.

4. Transparență și Responsabilitate

- **Transparență față de persoanele vizate**: În cazul solicitărilor privind protecția datelor (acces, rectificare, ștergere), registrul facilitează furnizarea rapidă de informații relevante.
- **Responsabilitate internă**: Demonstrează clar cine este responsabil de prelucrarea datelor și ce măsuri sunt implementate pentru a respecta obligațiile legale.

5. Eficiență în Gestionarea Controalelor sau Incidentelor

- În cazul unui control al ANSPDCP sau al unei breșe de securitate, registrul oferă documentația necesară pentru a arăta conformitatea cu GDPR și măsurile luate pentru prevenirea incidentelor similare.

6. Sprijin în Derularea Activităților Juridice

- **Litigii**: Registrul centralizează informațiile necesare privind datele prelucrate în cazuri juridice, ajutând la răspunsuri rapide și eficiente în instanță.

- **Contracte**: Asigură trasabilitatea datelor implicate în redactarea și gestionarea contractelor.

7. Evidențierea Responsabilului

Registrul identifică persoanele care intră în contact cu datele și responsabilul pentru gestionarea acestora în cadrul compartimentului juridic. Aceasta este o cerință obligatorie pentru respectarea **principiului responsabilității**.

8. Încurajarea Bunelor Practici

Registrul promovează bunele practici în ceea ce privește prelucrarea datelor:

- Prelucrare minimă a datelor necesare.
- Limitarea accesului doar la personalul autorizat.
- Asigurarea unui proces transparent și bine documentat.

.Exemple pentru Registrul de Evidență în Compartimentul Juridic

Nr	Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
1	Reprezentarea în instanță și soluționarea litigiilor	Nume, CNP, adresă, date de contact, informații despre dosar (plângeri, decizii, sentințe)	Părți implicate în litigii (angajați, colaboratori, terți)	Art. 6(1)(c): obligație legală; Art. 6(1)(e): interes public	Documentele fizice păstrate în dulapuri securizate; acces electronic limitat	3 ani după soluționarea definitivă a dosarului	Instanțe de judecată, avocați, executor judecătoresc	Arhiva fizică, server intern securizat	Consilier juridic, avocați desemnați
2	Redactarea,	Nume,	Angajați,	Art.	Stocare	10 ani	Curtea de	Server	Consilier

Nr	Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
	revizuirea și gestionarea contractelor	funcție, semnătură, date de contact	furnizori, colaboratori	6(1)(c): obligație legală; Art. 6(1)(e): interes public	criptată a documentelor pe server; acces controlat prin roluri	(Codul Civil, art. 944)	Conturi, ANAF	securizat, arhiva fizică	juridic, alte compartimente interne implicate
3	Oferirea de consultanță juridică internă	Nume, funcție, date relevante cazurilor juridice (plângeri, anchete)	Angajați, colaboratori, terți	Art. 6(1)(e): interes public	Notițele confidențiale păstrate în fișiere criptate	Până la finalizarea consultanței	N/A	Server securizat	Consilier juridic

Explicații Detaliate pentru Fiecare Coloană

1. **Scopul Prelucrării**:
   - Exemplu: "Reprezentarea juridică în litigiile cu angajați sau terți", "Gestionarea și arhivarea contractelor cu furnizorii", "Oferirea de consultanță juridică internă".
   - Scopurile sunt dictate de atribuțiile compartimentului juridic.
2. **Tipul de Date Colectate**:
   - Date de identificare: nume, prenume, CNP, adresă, telefon, e-mail.
   - Informații despre litigii: copii ale plângerilor, declarații, sentințe, dovezi.
   - Detalii contractuale: număr contract, părți implicate, obiectul contractului, termene.
3. **Persoane Vizate**:
   - Angajați implicați în litigii.
   - Colaboratori sau furnizori cu care sunt derulate contracte.

- Terți, cum ar fi persoane care au acționat instituția în judecată.

4. **Temei Legal**:
   - **Art. 6(1)(c)**: Obligație legală (ex. respectarea procedurilor judiciare).
   - **Art. 6(1)(e)**: Interes public (ex. asigurarea unei bune administrații și protecția drepturilor instituției).
5. **Măsuri de Securitate**:
   - **Fizice**: Documentele fizice păstrate în dulapuri securizate cu acces controlat.
   - **Tehnice**: Documente electronice stocate pe servere interne criptate, accesibile doar prin autentificare.
   - **Organizaționale**: Protocol strict pentru accesul la date, angajați instruiți privind confidențialitatea.
6. **Durata Păstrării**:
   - Documentele privind litigiile: 3 ani de la soluționarea definitivă a dosarului (Legea Arhivelor).
   - Contractele: 10 ani de la încetarea contractului (Codul Civil).
7. **Destinatari**:
   - **Interni**: Alți membri ai instituției implicați în proces (financiar, achiziții).
   - **Externi**: Instanțe de judecată, avocați, executor judecătoresc.
8. **Unde Stocăm Datele**:
   - **Fizic**: Arhiva compartimentului juridic (fișiere clasificate).
   - **Electronic**: Serverele interne protejate ale instituției, eventual un sistem de management al documentelor.
9. **Cine Intră în Contact cu Datele**:
   - Personalul juridic.
   - Alte departamente interne (ex. financiar, achiziții) în cazul contractelor sau documentelor relevante.
   - Avocați desemnați, în cazul reprezentării externe.

Exemple Specifice de Prelucrare

1. **Gestionarea Contractelor cu Furnizorii**:
   - Date prelucrate: date de identificare ale reprezentanților furnizorilor (nume, funcție, semnătură), obiectul contractului, durata.
2. **Reprezentarea în Instanță a Instituției**:
   - Date prelucrate: numele părților implicate, copii ale probelor, copii ale hotărârilor judecătorești.
3. **Soluționarea Litigiilor de Muncă**:
   - Date prelucrate: datele personale ale angajaților implicați, istoricul disciplinar, fișe de evaluare.

Concluzie

Registrul de evidență este un instrument indispensabil pentru compartimentul juridic, oferind atât conformitate legală, cât și un control eficient asupra datelor prelucrate. Prin documentarea completă și actualizată, instituția își protejează interesele juridice și demonstrează respectarea drepturilor persoanelor vizate, în conformitate cu GDPR

XII.5. Compartimentul IT (Informatica) al Serviciului de Ambulanță Județean Iași

Compartimentul IT (Informatica) al Serviciului de Ambulanță gestionează date esențiale pentru funcționarea și securitatea sistemelor informatice. Acest compartiment prelucrează în principal date tehnice, dar și date cu caracter personal pentru administrarea rețelelor, sistemelor și utilizatorilor. Iată cum se completează registrul de evidență pentru compartimentul IT:

Rolul Compartimentului IT în Prelucrarea Datelor cu Caracter Personal

Compartimentul IT (Informatica) joacă un **rol central** în prelucrarea datelor cu caracter personal, deoarece administrează infrastructura tehnică pe care se bazează toate activitățile instituției, inclusiv cele legate de gestionarea datelor sensibile. Acesta are responsabilitatea de a asigura confidențialitatea, integritatea și disponibilitatea datelor în sistemele informatice.

1. Administrarea și Securizarea Sistemelor IT

- **Configurarea și gestionarea conturilor de utilizator**: Compartimentul IT creează, administrează și șterge conturile utilizatorilor din sistemele informatice, asigurând că fiecare angajat are acces doar la datele relevante pentru activitatea sa.
- **Monitorizarea și prevenirea incidentelor de securitate**: IT-ul analizează log-urile de acces și alte activități din rețea pentru a detecta și preveni breșele de securitate.
- **Protecția datelor stocate**: Implementarea măsurilor de criptare, firewall-uri și backup-uri pentru a preveni pierderea datelor.

2. Suport Tehnic pentru Alte Departamente

- IT-ul este punctul de contact pentru raportarea problemelor tehnice legate de accesul la date sau de funcționarea aplicațiilor.
- În timpul suportului, acest compartiment poate avea acces temporar la datele utilizatorilor pentru diagnosticare, reparare sau restaurare.

3. Rol în Monitorizarea Conformității IT cu GDPR

- **Asigurarea respectării principiilor GDPR**: Compartimentul IT este responsabil pentru implementarea tehnologiilor care respectă cerințele GDPR, cum ar fi stocarea securizată a datelor și minimizarea prelucrărilor.

- **Implementarea drepturilor persoanelor vizate**: IT-ul sprijină alte departamente în furnizarea datelor solicitate de persoanele vizate (de exemplu, în cazul unei cereri de acces sau rectificare).

4. Gestiunea Incidențelor de Securitate

- În cazul unei breșe de securitate, IT-ul este responsabil de investigarea incidentului, identificarea cauzei și implementarea măsurilor corective.
- Documentarea detaliată a incidentelor și raportarea către DPO (Responsabilul cu Protecția Datelor).

Importanța Completării Registrului de Evidență

Registrul de evidență a prelucrării datelor este **esențial** pentru compartimentul IT, având următoarele roluri:

1. Transparență și Trasabilitate

- Registrul documentează fiecare proces de prelucrare a datelor realizat prin sistemele IT.
- Oferă trasabilitate pentru activitățile IT, indicând cine, când și cum prelucrează datele.

2. Conformitate cu „Articolul 30'' GDPR

- **Obligație legală**: Instituția este obligată să mențină un registru complet și actualizat al activităților de prelucrare. IT-ul contribuie prin documentarea detaliată a proceselor informatice care implică date personale.

3. Identificarea Riscurilor și Implementarea Măsurilor

- Registrul ajută la identificarea riscurilor asociate prelucrării datelor prin sisteme IT (breșe de securitate, acces neautorizat).

- Facilitează implementarea măsurilor tehnice și organizaționale adecvate pentru minimizarea riscurilor (criptare, autentificare, limitarea accesului).

4. Demonstrarea Conformității în Cazul unui Control

- Registrul este primul document solicitat de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) în cazul unui control.
- Un registru complet și actualizat demonstrează respectarea GDPR și reduce riscul sancțiunilor.

5. Protecția Datelor Sensibile

- Datele sensibile gestionate în sistemele IT (inclusiv datele pacienților, angajaților și log-urile de securitate) sunt protejate prin măsuri specifice Concluzie

Compartimentul IT este responsabil pentru protejarea datelor personale prin tehnologia și infrastructura instituției. Registrul de evidență joacă un rol vital în documentarea activităților IT, asigurând conformitatea cu GDPR și protejând datele împotriva riscurilor de securitate. Completarea corectă a registrului permite instituției să funcționeze eficient, să respecte drepturile persoanelor vizate și să evite sancțiuni.

Exemple pentru Registrul de Evidență în Compartimentul IT

Nr.	Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
1	Administrarea conturilor de utilizator și accesului la sistemele IT	Nume, prenume, ID utilizator, adrese IP, parole criptate, log-uri de	Angajați, colaboratori	Art. 6(1)(c): Obligație legală	Acces controlat prin autentificare în mai mulți pași, logarea accesului	Pe durata raportului de muncă + 1 an	N/A	Servere securizate interne	Personal IT autorizat

Nr.	Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
		acces							
2	Gestionarea sistemelor informatice și monitorizarea activității rețelei	Adrese IP, date de trafic, log-uri de sistem, detalii despre incidentele de securitate	Angajați, terți care accesează sistemele	Art. 6(1)(f): Interes legitim (securitate IT)	Monitorizare continuă, criptare, firewall-uri avansate	6 luni - 1 an (log-uri), conform politicii interne	N/A	Servere locale securizate, cloud intern	Personal IT
3	Suport tehnic pentru utilizatori	Nume, prenume, contact, detalii despre problemele tehnice raportate	Angajați	Art. 6(1)(c): Obligație legală; Art. 6(1)(e): Interes public	Înregistrări anonimizate după soluționare, stocare limitată	Până la soluționarea cererii + 6 luni	N/A	Servere securizate interne	Personal IT, coordonatori

Detalii pentru Fiecare Coloană

1. **Scopul Prelucrării**:
   - **Administrarea conturilor de utilizator**: Crearea, modificarea și eliminarea conturilor de acces în rețea și aplicațiile interne.
   - **Monitorizarea și securizarea rețelelor**: Prevenirea accesului neautorizat, detectarea și rezolvarea incidentelor de securitate.
   - **Suport tehnic**: Gestionarea problemelor raportate de utilizatori.
2. **Tipul de Date Colectate**:
   - **Date de identificare**: Nume, prenume, ID utilizator, adrese de e-mail.
   - **Date tehnice**: Adrese IP, log-uri de acces, date despre traficul de rețea.
   - **Informații despre incidente**: Erori de sistem, fișiere afectate, mesaje de eroare.

3. **Persoane Vizate**:
   - Angajați ai instituției.
   - Colaboratori externi care utilizează sistemele IT ale instituției.
   - Terți care interacționează cu sistemele, în cazul contractelor de suport sau întreținere IT.
4. **Temei Legal**:
   - **Art. 6(1)(c)**: Obligație legală (pentru respectarea normelor de securitate cibernetică).
   - **Art. 6(1)(f)**: Interes legitim (asigurarea funcționării și securității sistemelor).
5. **Măsuri de Securitate**:
   - **Tehnice**: Firewall-uri, criptare end-to-end, autentificare în mai mulți pași.
   - **Fizice**: Serverele fizice sunt amplasate în camere securizate.
   - **Organizaționale**: Proceduri stricte pentru acordarea accesului la date, revizuirea periodică a permisiunilor.
6. **Durata Păstrării**:
   - **Log-uri de acces**: 6 luni - 1 an, conform normelor interne și cerințelor legale.
   - **Date despre suport tehnic**: Până la soluționarea problemelor + 6 luni.
7. **Destinatari**:
   - **Interni**: Angajați din compartimentele juridic, administrativ sau conducere (pentru analiză sau investigare).
   - **Externi**: Autorități (ANSPDCP sau alte entități de supraveghere, în cazul investigațiilor).
8. **Unde Stocăm Datele**:
   - **Servere securizate**: Datele sunt stocate pe servere interne cu acces restricționat.
   - **Cloud privat**: Pentru backup sau partajare securizată.
9. **Cine Intră în Contact cu Datele**:
   - Personal IT autorizat.
   - Administratorii de sistem sau managerii IT.

- Consultanți sau furnizori de servicii IT externalizate, dacă este cazul.

Exemple Specifice de Prelucrare

1. **Gestionarea Parolelor Utilizatorilor**:
   - Date prelucrate: ID utilizator, parole criptate, adrese de e-mail.
   - Măsuri: Criptare AES pentru stocarea parolelor, autentificare în doi pași.
2. **Monitorizarea Rețelei**:
   - Date prelucrate: Adrese IP, log-uri de acces, alerte de securitate.
   - Măsuri: Sistem SIEM (Security Information and Event Management) pentru analiza log-urilor.
3. **Raportarea Problemelor IT**:
   - Date prelucrate: Nume utilizator, problemă raportată, soluție aplicată.
   - Măsuri: Înregistrări anonimizate după rezolvarea problemei.

XII.6. Compartimentul Financiar-Contabil;

Importanța Datelor Prelucrate

Compartimentul financiar-contabil gestionează o gamă largă de date cu caracter personal, care sunt esențiale pentru asigurarea conformității financiare, raportarea fiscală și respectarea obligațiilor legale ale instituției. Prelucrarea acestor date este fundamentală pentru funcționarea instituției, iar respectarea principiilor GDPR este crucială pentru protecția persoanelor vizate.

Tipuri de Date Prelucrate

1. **Datele angajaților:**
   - Nume și prenume.
   - Cod Numeric Personal (CNP).
   - Adresa de domiciliu.

- Date de contact (număr de telefon, adresă de e-mail).
- Date bancare (cont IBAN).
- Informații privind salariul, rețineri salariale, sporuri.
- Documente justificative (declarații fiscale, cereri de concediu, adeverințe).

2. **Datele furnizorilor și colaboratorilor:**
   - Nume și prenume ale reprezentanților furnizorilor persoane fizice sau PFA.
   - Date bancare pentru plăți.
   - CNP (unde este necesar pentru facturare sau alte raportări fiscale).
3. **Datele pacienților (în unele cazuri):**
   - Nume și prenume (pe facturi sau alte documente fiscale legate de servicii).
4. **Date financiare generale:**
   - Informații legate de plăți, creanțe, datorii.
   - Documente contabile care conțin date personale.

Cum se Completează Registrul de Evidență pentru Compartimentul Financiar-Contabil (Exemple)

Nr	Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
1	Deconturi cheltuieli, avansuri-Retineri. etc	Nume, CNP, date bancare, sporuri, rețineri salariale	Angajați	Art. 6(1)(c): Obligație legală	Acces controlat, date criptate în aplicații HR	Pe durata raportului de muncă + 50 ani	ITM, ANAF, bancă	Software de salarizare securizat	Personal contabil autorizat, conducerea instituției, secretariat

Nr	Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
2	Raportări fiscale și plăți către autorități	Nume, CNP, venituri, rețineri fiscale	Angajați	Art. 6(1)(c): Obligație legală	Documente fizice arhivate securizat, acces limitat	10 ani (arhivare legală)	ANAF, autorități fiscale	Servere interne securizate	Personal contabil autorizat, director economic, secretariat
3	Gestionarea relațiilorcu furnizorii	Nume, date bancare	Reprezentanți ai furnizorilor	Art. 6(1)(b): Executarea unui contract	Acces restricționat, documente criptate	Pe durata contractului + 5 ani	Banca, conducerea instituției	Arhivă fizică și electronică	Personal contabil, juridic
4	Emiterea documentelor contabile (facturi, chitanțe)	Nume, adrese, CNP (în cazuri specifice)	Angajați, pacienți, terți	Art. 6(1)(c): Obligație legală	Acces fizic și electronic securizat	10 ani	Autorități fiscale, instituții bancare	Servere securizate interne	Personal contabil
5	Gestionarea cererilor de deconturi	Nume, detalii financiare	Angajați	Art. 6(1)(b): Executarea unui contract	Politici clare de acces la documente	Pe durata raportului contractual + 5 ani	Conducerea instituției	Software securizat	Personal contabil

**In functie de datele procesate, scopul prelucrării, destinatarii datelor,relațiile dinte instituție și terți, etc. se va completa/actualiza/adapta registru de prelucre a datelor cu caracter personal.*

Detalii pentru Fiecare Secțiune

1. **Scopul Prelucrării**:
   - Gestionarea activităților financiare: calcul salarii, raportări fiscale, plăți către furnizori, emiterea de documente contabile.
   - Raportări și conformare legală cu legislația financiar-contabilă.
2. **Tipul de Date Colectate**:
   - Date de identificare (nume, CNP, adresă).
   - Date financiare (salarii, conturi bancare, plăți).
   - Date contractuale (informare și justificare).
3. **Persoane Vizate**:
   - Angajați.
   - Reprezentanți ai furnizorilor și colaboratori.
   - Pacienți (în cazuri specifice).
4. **Temei Legal**:
   - Art. 6(1)(c): Obligație legală (Codul Fiscal, Codul Muncii).
   - Art. 6(1)(b): Executarea unui contract (cu furnizorii sau colaboratorii).
5. **Măsuri de Securitate**:
   - **Tehnice**: Criptare, acces controlat la aplicațiile financiare, back-up periodic.
   - **Fizice**: Documente arhivate securizat, acces limitat la dosare fizice.
   - **Organizaționale**: Politici interne clare privind accesul la datele contabile.
6. **Durata Păstrării**:
   - 50 ani: Documentele de salarizare (conform legislației muncii).
   - 10 ani: Documente contabile, conform Codului Fiscal.
7. **Destinatari**:
   - ANAF, ITM, alte autorități fiscale sau de muncă.
   - Bănci, furnizori, conducerea instituției.
8. **Unde Stocăm Datele**:

- Arhive fizice securizate.
- Software financiar securizat.
- Servere interne cu acces controlat.

9. **Cine Intră în Contact cu Datele**:
   - Personal financiar-contabil autorizat.
   - Reprezentanți juridici (dacă este cazul).
   - Manageri IT (doar pentru aspectele tehnice legate de securitate).

Importanța Registrului de Evidență în Compartimentul Financiar-Contabil

1. **Conformitate cu legea**: Documentarea completă și actualizată asigură conformitatea cu Articolul 30 din GDPR și cu legislația financiar-contabilă.
2. **Gestionarea riscurilor**: Identifică riscurile asociate cu manipularea datelor financiare și permite aplicarea măsurilor de securitate.
3. **Evidența trasabilității**: Permite verificarea accesului și utilizării corecte a datelor financiare.
4. **Audit și control**: Registrul este un instrument de audit intern și extern, necesar pentru demonstrarea respectării obligațiilor legale.

XII.7. Compartimentul Mișcare și Exploatare Auto/Tehnic;

Importanța Datelor Prelucrate și Completarea Registrului

Compartimentul de Mișcare și Exploatare Auto / Tehnic are un rol esențial în gestionarea flotei de ambulanțe, asigurând funcționalitatea și siguranța acestora. Acest compartiment implică prelucrarea datelor cu caracter personal legate de utilizarea vehiculelor, personalul operativ, și, indirect, datele pacienților în contextul intervențiilor medicale.

PROCEDURĂ OPERAȚIONLĂ

Prelucrarea Datelor cu Caracter Personal în cadrul Serviciului de Ambulanță Județean Iași

GDPR

Importanța Datelor Prelucrate

1. **Asigurarea siguranței flotei auto**:
   - Gestionarea stării tehnice a vehiculelor pentru a respecta standardele de siguranță.
   - Coordonarea reviziilor și reparațiilor.
2. **Monitorizarea activității personalului operativ**:
   - Evidența șoferilor și a activității acestora (carnete de conducere, ore de lucru).
3. **Trasabilitatea datelor operaționale**:
   - Înregistrarea și gestionarea rutelor, foilor de parcurs și informațiilor legate de intervenții.
4. **Conformitatea legală**:
   - Respectarea reglementărilor privind utilizarea vehiculelor și protecția datelor personale ale pacienților transportați.

Date Prelucrate de Compartimentul Mișcare și Exploatare Auto

1. **Date despre șoferi și personalul tehnic**:
   - Nume și prenume.
   - CNP, seria și numărul permisului de conducere.
   - Calificări și atestări.
   - Ore de lucru, ture, evidența prezenței.
   - Date de contact (telefon, e-mail).
2. **Date despre vehicule**:
   - Date de identificare (număr de înmatriculare, seria șasiului).
   - Istoric tehnic al vehiculului (reparații, revizii, ITP).
   - Monitorizare prin GPS (în cazul utilizării).
3. **Date despre pacienți (indirect)**:
   - Înregistrate în contextul transportului medical (nume, stare medicală, traseu, orar).
4. **Date despre intervenții**:

- Date operaționale (rute, consumuri de combustibil, timp de intervenție).

Cum se Completează Registrul de Evidență pentru Compartimentul Mișcare și Exploatare Auto (Exemple)

Nr.	Scopul Prelucrării	Tipul de ate Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
1	Gestionarea rilor și flotei auto	Nume, permis onducere, ore ucru	Șoferi	Art.)(c): igație lă	Acces limitat aza de date, puri rizate	Pe durata angajării + 3 ani	Manager tehnic, DPO	Arhivă fizică și server intern	Personal autorizat
2	Monitorizarea lor și activității iculelor	Date GPS, ee, ore de u	Șoferi, enți irect)	Art.)(e): Interes lic; Art.)(h): ătate	Date tate, acces ricționat	3 ani	IT, conducerea instituției	Server intern și dispozitive GPS	Manager tehnic
3	Gestionarea vităților de ținere	Date vehicule bric tehnic, năr atriculare)	Personal lic, izori	Art.)(b): cutarea i contract	Evidențe e în arhive rizate	Durata utilizării vehiculului + 3 ani	Manager tehnic, juridic	Arhivă tehnică securizată	Personal tehnic
4	Transportul enților	Date pacienți me, traseu, ea medicală)	Pacienți	Art.)(e): Interes lic; Art.)(h): ătate	Sisteme tate, acces tat	5 ani conform reglementărilor	Medicii coordonatori, DPO	Server și arhive electronice	Personal operativ autorizat

Explicații pentru Completarea Fiecărei Secțiuni

Scopul Prelucrării

- Gestionarea și întreținerea vehiculelor pentru intervenții.
- Monitorizarea utilizării flotei auto.

- Respectarea reglementărilor de siguranță rutieră și de operare.
- Transportul și îngrijirea pacienților.

Tipuri de Date Colectate

- Datele personale ale șoferilor, pacienților și furnizorilor, preluate pentru operarea eficientă a flotei și asigurarea serviciilor medicale.

Persoane Vizate

- Șoferi și personal tehnic.
- Pacienți transportați de ambulanțe.
- Furnizori de servicii tehnice sau echipamente.

Temei Legal

- **Art. 6(1)(c)**: Obligația legală de gestionare a datelor operaționale.
- **Art. 6(1)(b)**: Executarea contractelor cu furnizorii.
- **Art. 6(1)(e)**: Interes public, pentru buna funcționare a serviciilor medicale.
- **Art. 9(2)(h)**: Prelucrarea datelor sensibile pentru asistență medicală.

Măsuri de Securitate

- Sisteme de monitorizare GPS protejate prin autentificare.
- Arhivare fizică în spații securizate (fișiere tehnice, foi de parcurs).
- Protecția electronică a datelor (criptare și acces limitat).

Durata Păstrării

- Datele despre activitatea vehiculelor și șoferi: pe durata utilizării vehiculului + 3 ani.
- Datele pacienților: conform legislației medicale, de obicei 5 ani.

- Datele furnizorilor: durata contractului + 5 ani.

Destinatari

- Conducerea instituției pentru raportare.
- Departamentul IT pentru gestionarea și securizarea datelor electronice.
- Juridicul, pentru verificări în cazuri de litigi.

Unde Stocăm Datele

- Arhive fizice pentru foi de parcurs și evidențe tehnice.
- Servere interne securizate pentru loguri și date GPS.

Cine Intră în Contact cu Datele

- Personal autorizat din cadrul compartimentului tehnic și IT.
- Manageri responsabili și DPO.

Importanța Completării Registrului

- **Conformitate**: Registrul asigură respectarea GDPR și a reglementărilor interne.
- **Trasabilitate**: Permite identificarea activităților și responsabilităților în gestionarea datelor.
- **Reducerea riscurilor**: Oferă o bază pentru evaluarea și prevenirea riscurilor asociate.
- **Transparență**: Creează o imagine clară asupra modului de gestionare a datelor în cadrul compartimentului.

XII.8. Compartiment Medical

Registrul de prelucrare a datelor cu caracter personal este un document esențial în cadrul compartimentului medical al Serviciului de Ambulanță Județean Iași, având rolul de a asigura conformitatea cu reglementările GDPR și protecția datelor pacienților. Completarea corectă și actualizarea acestuia sunt cruciale pentru respectarea normelor legale și pentru protejarea informațiilor sensibile cu caracter personal.

Principalele motive pentru care acest registru este important în compartimentul medical:

1. **Asigurarea Conformității cu GDPR**

Fiecare activitate de prelucrare a datelor personale trebuie documentată, iar registrul este instrumentul prin care se demonstrează conformitatea cu cerințele GDPR. În compartimentul medical, acesta include datele sensibile ale pacienților și, prin urmare, necesită o gestionare strictă și bine documentată.

2. **Transparența Prelucrării Datelor**

Registrul ajută la asigurarea transparenței prelucrării datelor, indicând tipurile de date prelucrate, scopul prelucrării și temeiul legal pentru fiecare activitate de prelucrare. Acest lucru este esențial pentru a putea răspunde solicitărilor pacienților sau autorităților.

3. **Măsuri de Protecție a Datelor Pacienților**

În cadrul compartimentului medical, datele sensibile ale pacienților trebuie protejate cu rigurozitate. Registrul ajută la identificarea măsurilor de protecție, precum criptarea datelor sau restricționarea accesului la acestea, pentru a preveni orice risc de acces neautorizat.

4. **Clarificarea Responsabilităților**

Registrul detaliază cine are acces la datele pacienților și care sunt responsabilitățile fiecărei persoane implicate în prelucrarea acestora. În compartimentul medical, acest lucru este crucial pentru a asigura un management corect al datelor și pentru a preveni erori sau încălcări ale legislației.

5. **Identificarea Riscurilor Asociate Prelucrării Datelor**

Registrul permite identificarea și evaluarea riscurilor ce pot apărea în procesul de prelucrare a datelor, astfel încât să se poată implementa măsuri adecvate de protecție și prevenire a breșelor de securitate.

6. **Audit și Control Intern**

În cadrul compartimentului medical, registrul servește și ca bază pentru audituri interne, care garantează că prelucrarea datelor este realizată corect și conform procedurilor stabilite, asigurând transparența și responsabilitatea continuă.

7. **Documentarea Proceselor de Prelucrare**

Registrul permite documentarea detaliată a activităților de prelucrare, inclusiv motivele prelucrării, scopurile și temeiurile legale. Acesta ajută la clarificarea și justificarea fiecărei prelucrări de date, ceea ce este esențial în caz de audit sau solicitări din partea pacienților.

1. Scopul Prelucrării

- **Compartiment Medical**:
  - Asigurarea asistenței medicale și salvarea vieții pacientului.
  - Gestionarea istoricului medical pentru tratamente ulterioare.
  - Raportări obligatorii către autorități (statistici,etc).
- **Dispecerat**:
  - Preluarea apelurilor de urgență și coordonarea echipajelor.

- Ghidarea intervenției în funcție de specificul urgenței.

- **Echipaje de Intervenție**:
  - Colectarea informațiilor pentru diagnostic rapid și tratament.
  - Documentarea intervenției pentru continuitatea îngrijirii medicale.

2. Tipul de Date Colectate

- **Compartiment Medical**:
  - Date de identificare (nume, CNP, adresă).
  - Date sensibile (diagnostic, istoricul medical, tratamente).
- **Dispecerat**:
  - Datele apelantului (nume, telefon).
  - Date despre pacient (simptome, locația incidentului).
- **Echipaje de Intervenție**:
  - Datele pacientului (nume, diagnostic prezumtiv).
  - Date medicale (tensiune arterială, glicemie, alte valori măsurate).

3. Persoane Vizate

- **Compartiment Medical**:
  - Pacienți tratați în cadrul serviciului.
  - Aparținători (în cazuri de minori sau persoane inconștiente).
- **Dispecerat**:
  - Apelanți și pacienți.
- **Echipaje de Intervenție**:
  - Pacienți preluați.
  - Aparținători care oferă detalii despre pacient.

4. Temeiul Legal

- **Art. 6(1)(d)**: Protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice.
- **Art. 6(1)(c)**: Îndeplinirea unei obligații legale.
- **Art. 9(2)(h)**: Prelucrarea datelor sensibile pentru furnizarea de asistență medicală sau tratament.

5. Măsuri de Securitate

- **Fizice**:
  - Arhive securizate cu acces limitat.
  - Fișele medicale transportate sigilat.
- **Tehnice**:
  - Acces restricționat pe bază de autentificare (parole, carduri de acces).
  - Backup periodic al datelor electronice.
- **Organizaționale**:
  - Instruirea periodică a personalului cu privire la protecția datelor.
  - Proceduri interne pentru raportarea încălcărilor de securitate.

6. Durata de Păstrare a Datelor

- **Compartiment Medical**:
  - Fișele medicale: minim 5 ani, conform legislației naționale (ex. Legea 95/2006).
- **Dispecerat**:
  - Înregistrările apelurilor: 3 ani (sau conform legislației aplicabile).
- **Echipaje de Intervenție**:
  - Fișele de intervenție: minim 5 ani.

7. Cine Intră în Contact cu Datele

- **Compartiment Medical**: Medici, asistente, personal administrativ.
- **Dispecerat**: Dispecerii, operatorii care preiau apelurile.
- **Echipaje de Intervenție**: Personalul de pe ambulanță (medici, asistenți, paramedici).

8. Categorii de Destinatari

- **Interne**: Personal medical, echipe de intervenție, dispeceri.
- **Externe**: Spitale, autorități publice (ex. DSP), poliție, ISU.

9. Unde Stocăm Datele

- **Fizic**: Arhive securizate din cadrul instituției.
- **Electronic**: Servere protejate prin sisteme de autentificare și criptare.

10. Riscul Asociat Prelucrării

- **Riscuri Posibile**:
  - Acces neautorizat la date.
  - Pierderea fișelor fizice.
  - Breșe de securitate în sistemele IT.
- **Măsuri de Reducere a Riscului**:
  - Monitorizarea accesului la date.
  - Backup periodic al datelor electronice.
  - Distrugerea fișelor fizice conform legislației.

11. Persoana Responsabilă la Nivel de Departament

- Fiecare compartiment desemnează un responsabil (medicul coordonator, șeful de dispecerat, etc.).

- Decizia trebuie emisă printr-un act administrativ al instituției.

Exemplu 1: Compartimentul Medical

Scopul elucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
Asigurarea asistenței medicale pentru pacienți	Nume, CNP, adresă, diagnostic, tratamente aplicate	Pacienți, aparținători	Art. 6(1)(c); Art. 9(2)(h)	Fișele păstrate în dulapuri închise, acces electronic prin parole	5 ani	Spitale, autorități medicale	Arhiva fizică, server securizat	Medici, asistente, personal administrativ

Exemplu 2: Dispecerat

Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intră în Contact cu Datele
Coordonarea apelurilor de urgență	Nume apelant, telefon, locația pacientului, simptome	Apelanți, pacienți	Art. 6(1)(d); Art. 9(2)(h)	Sisteme de apel securizate, înregistrare protejată prin acces controlat	3 ani	Echipaje, ISU, Poliție, DSP	Sistem electronic de gestionare a apelurilor	Dispeceri, operatori de urgență

Exemplu 3: Echipaje de Intervenție

Scopul Prelucrării	Tipul de Date Colectate	Persoane Vizate	Temei Legal	Măsuri de Securitate	Durata Păstrării	Destinatari	Unde Stocăm Datele	Cine Intr în Contact cu Datel
Realizarea intervențiilor medicale și asigurarea continuității tratamentului	Nume, vârstă, diagnostic, tratamente aplicate	Pacienți, aparținători	Art. 6(1)(d); Art. 9(2)(h)	Păstrarea fișelor fizice în plicuri sigilate, transmitere electronică criptată	5 ani	Spitale, autorități medicale	Arhiva fizică, dispozitive mobile securizate	Medici, asistenți, paramedi

Exemplu 4: Prelucrarea datelor pacienților pentru intervențiile medicale de urgență

Tipul de date	Scopul prelucrării	Temeiul legal	Categorie destinatari	Unde stocăm datele	Cine intră în contact cu datele	Risc	Persoana responsabilă la nivel de birou
Date de identificare (Nume, Prenume, CNP, Adresă) și date medicale (istoric medical, diagnostic, tratamente)	Intervenții medicale de urgență la locul accidentului și în timpul transportului la spital	Art. 6(1)(d) – Prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate	Spitale, medici de la spitalul de urgență, echipele medicale de intervenție	Serverele interne ale Serviciului de Ambulanță Județean	Dispecerii și echipajele medicale	Riscul accesului neautorizat sau pierderea datelor sensibile	Medicul coordonator al echipajului de urgență

Exemplu 5: Prelucrarea datelor pacienților pentru prevenirea abuzului și

gestionarea pacienților vulnerabili

Tipul de date	Scopul prelucrării	Temeiul legal	Categorie destinatari	Unde stocăm datele	Cine intră în contact cu datele	Risc	Persoana responsabilă la nivel de birou
Date de identificare și istoricul medical complet (diagnostic, tratamente)	Identificarea pacienților vulnerabili și prevenirea abuzului sau a neglijenței	Art. 6(1)(e) – Prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public	Serviciile de protecția copilului, autoritățile judiciare, medici de specialitate	Fișierele electronice și fizice ale Serviciului de Ambulanță	Personalul medical implicat în evaluarea și raportarea cazurilor	Riscul de divulgare a informațiilor sensibile către persoane neautorizate	Coordonatorul echipajului și medicii specializați

Coloane Detaliate

1. **Scopul Prelucrării**:
   - Detalii clare despre motivul procesării: "Gestionarea apelurilor de urgență", "Asigurarea tratamentului medical".
2. **Tipul de Date Colectate**:
   - Specificați exact ce fel de date sunt implicate: date de identificare (nume, prenume), date sensibile (diagnostic, tratament).
3. **Persoane Vizate**:
   - Includeți categorii generale (pacienți, apelanți, aparținători).
4. **Temei Legal**:
   - Precizați articolele aplicabile din GDPR, cum ar fi Art. 6(1)(c) și Art. 9(2)(h).
5. **Măsuri de Securitate**:
   - Detalii tehnice și organizaționale, cum ar fi criptarea datelor, arhivare securizată, acces restricționat.
6. **Durata Păstrării**:
   - Specificați durata în funcție de reglementările naționale: ex. "3 ani pentru înregistrările apelurilor, 5 ani pentru fișele medicale".

7. **Destinatari**:
   - Listează entitățile interne sau externe care pot accesa datele: spitale, autorități de reglementare, poliție.
8. **Unde Stocăm Datele**:
   - Clarificați locația stocării: arhivă fizică, servere securizate, aplicații de gestionare a apelurilor.
   - **Cine Intră în Contact cu Datele**:
   - Includeți funcțiile și rolurile specifice: dispeceri, medici, asistente, echipaj de intervenție.

XI.9. Compartimentul/ biroul statistică din cadrul SAJ Iași;

1. Rolul compartimentului/biroului statistică în prelucrarea datelor cu caracter personal:

Compartimentul de statistică în cadrul Serviciului de Ambulanță Iași (SAJ), joacă un rol important în prelucrarea datelor cu caracter personal, mai ales în contextul respectării reglementărilor privind protecția datelor (precum Regulamentul (UE) 2016/679 – GDPR). Acesta are mai multe responsabilități, printre care:

a. **Colectarea și analiza datelor**: Compartimentul de statistică poate colecta și analiza datele cu caracter personal pentru a evalua eficiența serviciilor prestate, tendințele de intervenție, numărul de apeluri, tipurile de urgențe și alte aspecte relevante. Aceste statistici pot ajuta la optimizarea resurselor și îmbunătățirea serviciilor.
b. **Confidențialitate și protecția datelor**: Chiar și în scopuri statistice, compartimentul trebuie să se asigure că datele cu caracter personal sunt tratate în conformitate cu reglementările privind protecția datelor. De obicei, datele vor fi anonimizate sau pseudonimizate pentru a preveni identificarea directă a persoanelor.

c. **Raportarea și transmiterea datelor**: Compartimentul de statistică poate fi responsabil de pregătirea și transmiterea rapoartelor periodice sau a datelor statistice către autoritățile competente, precum Ministerul Sănătății, în scopul monitorizării și planificării serviciilor de urgență.

d. **Respectarea reglementărilor interne**: Compartimentul trebuie să respecte normele interne stabilite în cadrul SAJ pentru prelucrarea datelor cu caracter personal și să colaboreze cu echipele de protecția datelor, pentru a se asigura că datele colectate sunt utilizate în mod legal și etic.

2. Exemple de date prelucrate

- **Exemplu**: Biroul de statistică poate colecta informații legate de numărul de intervenții efectuate într-o anumită perioadă (de exemplu, lunar sau anual), tipurile de urgențe (accidente, atacuri de cord, accidente rutiere), zonele geografice în care au avut loc aceste intervenții, vârsta și sexul pacienților.
- **Prelucrare**: Aceste date pot fi utilizate pentru a crea rapoarte interne sau externe despre activitatea SAJ și pentru a analiza tendințele și eficiența serviciului.

Crearea de statistici agregate privind tipurile de intervenții:

- **Exemplu**: Biroul de statistică poate prelucra date despre tipul și frecvența apelurilor primite, tipurile de afecțiuni tratate (cum ar fi urgențele cardiace, accidente de muncă, urgențe pediatrice).
- **Prelucrare**: Datele pot fi agregate și anonimizate pentru a obține statistici care pot fi folosite pentru analiza resurselor necesare și pentru pregătirea personalului.

Monitorizarea performanței echipajelor de intervenție:

- **Exemplu**: Biroul de statistică poate analiza timpul de răspuns al echipajelor, de la primirea apelului până la ajungerea la pacient, pentru a evalua eficiența și timpii de reacție.

- **Prelucrare**: Datele pot include informații despre locațiile intervențiilor și timpii de răspuns, iar acestea sunt prelucrate pentru a optimiza resursele și timpii de intervenție.

□ **Analiza impactului sezonier al intervențiilor**:

- **Exemplu**: Biroul de statistică poate analiza datele pentru a observa dacă există fluctuații sezoniere ale apelurilor de urgență (de exemplu, creșteri în perioada de iarnă din cauza accidentelor de circulație sau afecțiunilor respiratorii).
- **Prelucrare**: Datele cu caracter personal ale pacienților pot fi folosite pentru a înțelege mai bine cerințele sezoniere și pentru a ajuta la planificarea resurselor și personalului în perioadele de vârf.

3. Cadru legal

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (GDPR). Iată principalele acte normative care reglementează această activitate:

1. **Regulamentul (UE) 2016/679 (GDPR)**:
    - **Articolul 6 - Legalitatea prelucrării**: Prelucrarea datelor personale de către biroul de statistică trebuie să fie realizată pe baza unuia dintre temeiurile legale prevăzute de GDPR. De exemplu, prelucrarea poate fi justificată prin interesul public, îndeplinirea unei sarcini legale sau a unei obligații de serviciu public.
    - **Articolul 9 - Prelucrarea categoriilor speciale de date personale**: Dacă biroul de statistică prelucrează date sensibile (cum ar fi datele privind sănătatea), este necesar să aplice măsuri suplimentare de protecție, având în vedere că astfel de date necesită condiții mai stricte pentru prelucrarea lor.
    - **Articolul 5 - Principiile prelucrării datelor**: Prelucrarea trebuie să fie efectuată în mod legal, echitabil și transparent, să fie colectate pentru scopuri specifice și

legitime, și să fie păstrate doar pentru perioada necesară scopurilor pentru care au fost colectate.

- **Articolul 32 - Securitatea prelucrării**: Biroul de statistică trebuie să asigure măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva accesului neautorizat, pierderii sau distrugerii.

2. **Legea nr. 190/2018 privind măsurile de aplicare a GDPR în România**:
   - Aceasta reglementează specific modalitățile de implementare a GDPR în România și include norme suplimentare privind prelucrarea datelor personale în scopuri statistice.
   - În contextul activității biroului de statistică, legea prevede că prelucrarea datelor în scopuri statistice poate fi realizată chiar și fără consimțământul persoanei, dar cu respectarea unor măsuri adecvate de protecție a datelor (de exemplu, anonimizarea sau pseudonimizarea datelor).
3. **Legea nr. 677/2001 privind protecția datelor cu caracter personal și libera circulație a acestora** (abrogată, dar încă relevantă pentru contextul românesc):
   - Această lege a fost înlocuită de GDPR, dar a reprezentat fundamentul prelucrării datelor în România înainte de 2018. Multe dintre principiile reglementate de această lege sunt acum integrate în GDPR.
4. **Ordinul nr. 52/2006 privind organizarea și funcționarea birourilor de statistică**:
   - Deși nu reglementează direct protecția datelor cu caracter personal, acest ordin definește cadrul organizatoric pentru activitatea birourilor de statistică, care trebuie să fie în conformitate cu reglementările privind protecția datelor atunci când colectează și prelucrează date.
5. **Codul de Etică și Conduită în domeniul statisticii publice**:
   - În cadrul activității de statistică, inclusiv a birourilor de statistică din cadrul SAJ Iasi, este important să se urmeze un cod de etică care subliniază importanța protecției datelor și respectării drepturilor persoanelor vizate.

Scopul prelucrării

PROCEDURĂ OPERAȚIONLĂ

Prelucrarea Datelor cu Caracter Personal în cadrul Serviciului de Ambulanță Județean Iași

GDPR

Scopul prelucrării datelor cu caracter personal în cadrul compartimentului de statistică în Serviciu de Ambulanță Iași (SAJ) este de a colecta, analiza și utiliza datele pentru a obține informații și statistici utile, care contribuie la îmbunătățirea eficienței, calității și planificării serviciilor de urgență. Mai exact, scopurile prelucrării includ:

1. **Analiza activității și performanței**:
   - **Scop**: Colectarea și prelucrarea datelor pentru a evalua performanța echipajelor și eficiența serviciilor. De exemplu, se analizează timpii de răspuns, numărul și tipologia intervențiilor, zonele cele mai afectate de apeluri, pentru a înțelege unde sunt necesare îmbunătățiri.
2. **Crearea de statistici pentru managementul resurselor**:
   - **Scop**: Prelucrarea datelor pentru a sprijini luarea deciziilor în ceea ce privește alocarea resurselor (echipaje, ambulanțe, personal), bazându-se pe analiza volumului și tipului de intervenții.
3. **Monitorizarea tendințelor și identificarea problemelor de sănătate publică**:
   - **Scop**: Prelucrarea datelor pentru a identifica tendințele în intervențiile de urgență, cum ar fi frecvența anumitor tipuri de cazuri (accidente, atacuri de cord, urgențe pediatrice), care pot ajuta la planificarea măsurilor de prevenire a problemelor de sănătate publică.
4. **Raportarea către autoritățile competente**:
   - **Scop**: Generarea de rapoarte statistice care sunt trimise către Ministerul Sănătății, autoritățile locale sau alte instituții pentru a reflecta activitatea și pentru a ajuta la monitorizarea și îmbunătățirea serviciilor de urgență.
5. **Evaluarea impactului sezonier sau geografic**:
   - **Scop**: Prelucrarea datelor pentru a evalua fluctuațiile sezoniere (de exemplu, creșterea apelurilor în sezonul rece din cauza problemelor respiratorii sau a accidentelor de circulație) sau pentru a analiza concentrarea apelurilor în anumite zone geografice.

6. **Sprijinirea planificării strategice și a formării personalului**:
    - **Scop**: Utilizarea datelor statistice pentru a sprijini dezvoltarea unor strategii pe termen lung, inclusiv necesitățile de formare pentru personalul medical, echipaje, precum și investițiile în infrastructură.
7. **Asigurarea respectării reglementărilor și îmbunătățirea serviciilor**:
    - **Scop**: Prelucrarea datelor pentru a monitoriza conformitatea cu standardele și reglementările de sănătate publică, și pentru a identifica zonele în care serviciile ar putea fi îmbunătățite.

4. **Tipuri de Date Colectate**

1. Date de identificare a pacientului (date cu caracter personal)

- **Exemple**: Numele, prenumele, adresa, data nașterii, numărul de telefon.
- **Scop**: Deși aceste date sunt necesare pentru gestionarea intervenției și contactarea pacientului, ele sunt folosite mai puțin pentru analizele statistice propriu-zise, dar pot fi necesare pentru a asigura că statistica este completă și corectă.

2. Date despre tipologia intervențiilor

- **Exemple**: Tipul urgenței (de exemplu, accident rutier, atac de cord, traumatisme, urgențe pediatrice), codul medical al urgenței (în funcție de sistemul de triere utilizat).
- **Scop**: Aceste date sunt esențiale pentru analiza tipurilor de cazuri gestionate de SAJ, pentru a înțelege distribuția cazurilor și pentru a adapta resursele în funcție de cerințele fiecărui tip de urgență.

3. Date geografice (locația intervenției)

- **Exemple**: Adresa de intervenție, zona de acoperire (de exemplu, un anumit sector sau localitate), coordonatele GPS.

- **Scop**: Aceste date sunt importante pentru analiza distribuției geografice a intervențiilor și pentru evaluarea eficienței acoperirii teritoriale a serviciului de ambulanță.

4. Date despre echipajele de intervenție

- **Exemple**: Tipul echipajului (medic, paramedic, asistent), numărul echipajului, timpul de răspuns.
- **Scop**: Aceste date ajută la analiza performanței echipajelor de intervenție, evaluarea timpilor de răspuns și alocarea eficientă a resurselor.

5. Date temporale

- **Exemple**: Ora primirii apelului, timpul de plecare al ambulanței, timpul de ajungere la pacient, durata intervenției.
- **Scop**: Datele temporale sunt esențiale pentru analiza eficienței serviciului, inclusiv pentru monitorizarea respectării termenelor de răspuns și identificarea potențialelor îmbunătățiri.

6. Date despre starea pacientului la momentul intervenției

- **Exemple**: Starea pacientului (de exemplu, conștient, inconștient), evaluarea medicală la fața locului, necesitatea transportului la spital.
- **Scop**: Aceste informații sunt utile pentru analiza tipurilor de intervenții necesare și pentru ajustarea protocolului medical, în funcție de severitatea cazului.

7. Date despre transport și destinația pacientului

- **Exemple**: Spitalul către care a fost transportat pacientul, distanța până la unitatea medicală, tipul de spital (de urgență, specializat etc.).
- **Scop**: Aceste date sunt importante pentru analiza capacității spitalelor de a primi pacienți și pentru a evalua timpul de transport.

8. Date statistice agregate

- **Exemple**: Numărul total de intervenții pe tipuri de urgență, numărul de apeluri pe lună, datele agregate despre vârstă și sexul pacienților.
- **Scop**: Aceste date sunt utilizate pentru a crea statistici care ajută la planificarea serviciilor și la evaluarea performanței generale a SAJ.

9. Date despre echipamentele utilizate

- **Exemple**: Tipul echipamentelor medicale utilizate (de exemplu, defibrilator, oxigenoterapie), consumabilele utilizate în timpul intervenției.
- **Scop**: Datele referitoare la echipamente sunt colectate pentru a monitoriza utilizarea și necesarul de resurse materiale pentru intervenții.

10. Date privind rezultatele intervenției

- **Exemple**: Starea pacientului la finalizarea intervenției (de exemplu, îmbunătățire, agravare, decedat), recomandările făcute (spitalizare, urmărire etc.).
- **Scop**: Aceste date ajută la analiza rezultatelor intervențiilor și la evaluarea eficienței și calității serviciilor prestate.

11. Date administrative

- **Exemple**: Tipul serviciului solicitat (urgență, transport non-urgent), informații despre apelul telefonic (de exemplu, numărul apelantului).
- **Scop**: Aceste date sunt utile pentru gestionarea apelurilor și pentru rapoartele administrative legate de activitatea SAJ.

5. Destinatarii Datelor

Destinatarii datelor colectate de compartimentul de statistică din cadrul Serviciului de Ambulanță (SAJ) pot include atât entități interne, cât și externe, care au un interes legitim în utilizarea acestor date pentru diverse scopuri administrative, de planificare, raportare și îmbunătățire a serviciilor. Cu toate acestea, pentru a respecta legislația privind protecția datelor cu caracter personal, fiecare transfer de date trebuie să fie realizat în conformitate cu principiile prevăzute de **Regulamentul (UE) 2016/679 (GDPR)** și să se asigure că protecția datelor este menținută.

Posibilii destinatari ai datelor în cadrul compartimentului/biroului de statistică:

1. Entități interne din cadrul SAJ

- **Managerii și echipele de coordonare**: Datele colectate pot fi folosite de manageri pentru a monitoriza performanța echipajelor, a analiza eficiența intervențiilor și a lua decizii strategice privind resursele și operarea serviciilor.
- **Departamentele administrative**: Aceste date pot fi accesate de departamentele de resurse umane, logistică sau IT pentru gestionarea personalului, planificarea echipamentelor și infrastructurii.
- **Echipajele de intervenție**: Anumite date pot fi accesibile echipajelor de ambulanță pentru a pregăti intervențiile și a asigura un răspuns adecvat (de exemplu, istoricul intervențiilor pentru un pacient sau tipologia cazului).

2. Autoritățile de reglementare și instituțiile guvernamentale

- **Ministerul Sănătății și alte autorități publice**: Datele agregate și rapoartele statistice pot fi transmise către autoritățile naționale sau locale pentru a evalua performanța serviciilor de urgență și a planifica măsuri de îmbunătățire a sistemului de sănătate publică.
- **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**: În cazul în care există preocupări privind conformitatea cu GDPR sau alte

reglementări, ANSPDCP poate solicita informații legate de prelucrarea datelor cu caracter personal.

3. Spitale și unități medicale

- **Spitale și clinici**: Datele despre pacient pot fi transmise către spitale, dacă este necesar pentru continuarea îngrijirii medicale, cum ar fi transportul pacientului la spital sau furnizarea unor informații medicale despre starea pacientului.
- **Unități de primiri urgențe**: În funcție de tipul de intervenție, datele pacientului pot fi trimise unităților de primiri urgențe (UPU) pentru a asigura continuitatea tratamentului.

4. Asigurători de sănătate

- **Companii de asigurări**: În cazurile în care pacientul este asigurat și este necesar pentru procesul de rambursare a cheltuielilor, anumite date pot fi transmise asigurătorilor pentru a justifica costurile legate de serviciile prestate.

5. Entități de cercetare și instituții academice

- **Universități și instituții de cercetare**: Datele anonimizate sau agregate pot fi utilizate pentru cercetări academice și studii științifice legate de sănătatea publică, intervențiile de urgență, analiza tendințelor în domeniul medical, etc. În astfel de cazuri, este esențial ca datele să fie anonimizate pentru a respecta confidențialitatea pacienților.

6. Furnizori de servicii externe

- **Furnizori de servicii IT**: Dacă sunt utilizate soluții externe pentru stocarea datelor, prelucrarea lor sau gestionarea rapoartelor, acești furnizori vor avea acces la datele necesare pentru prestarea serviciilor. În acest caz, este necesar să existe un **contract de procesare a datelor** între SAJ și furnizorii respectivi, conform prevederilor GDPR.

- **Consultanți și auditori externi**: În cazul unor audite interne sau externe, sau al unui proces de îmbunătățire a serviciilor, datele pot fi puse la dispoziția auditoriilor sau consultanților pentru analiza performanței SAJ.

7. Publicul larg (în anumite condiții)

- **Datele agregate publice**: În anumite cazuri, datele agregate (anonimizate) pot fi publicate pentru a oferi informații despre activitatea SAJ, cum ar fi statistici privind numărul total de intervenții, tipurile de cazuri, timpul mediu de răspuns etc. Aceste date nu trebuie să conțină informații care ar putea identifica persoane.

8. Autorități judiciare și alte entități publice

- **Curțile de Justiție și alte autorități legale**: În cazuri speciale, datele cu caracter personal pot fi furnizate autorităților judiciare sau altor entități publice, dacă acest lucru este cerut prin lege sau pentru a respecta o obligație legală.

Protecția datelor în transferul acestora

În toate cazurile menționate mai sus, transferul datelor trebuie să fie realizat într-un mod care asigură respectarea drepturilor persoanelor vizate și protecția datelor. Acest lucru înseamnă, printre altele, utilizarea unor mecanisme de securitate adecvate, cum ar fi criptarea datelor și acorduri legale (de exemplu, acorduri de procesare a datelor) între S.A.J. Iași și destinatarii externi.

9. Perioada de Păstrare a Datelor

În România, perioada de păstrare a datelor cu caracter personal prelucrate în cadrul compartimentului de statistică al Serviciului de Ambulanță Iași (SAJ) este reglementată de **Regulamentul (UE) 2016/679 (GDPR)** și de legislația națională referitoare la protecția datelor cu caracter personal. Conform acestor reglementări, datele cu caracter personal trebuie să fie păstrate pentru o perioadă care nu depășește **perioada necesară scopurilor pentru care au fost colectate.**

În cazul specific al compartimentului de statistică din S.A.J Iași, termenul de păstrare a datelor depinde de mai mulți factori, precum tipul de date, scopul prelucrării și reglementările specifice din domeniul sănătății publice.

10.Aspecte relevante pentru perioada de păstrare:

1. **Principiul limitării stocării (Art. 5 GDPR)**:
   - Datele cu caracter personal trebuie păstrate doar atât timp cât sunt necesare scopurilor pentru care au fost colectate și prelucrate. După atingerea scopurilor respective, datele trebuie șterse sau anonimizate.
2. **Perioade legale de păstrare**:
   - În domeniul sănătății, legislația națională (cum ar fi Legea nr. 95/2006 privind reforma în domeniul sănătății) și reglementările specifice pot impune termene de păstrare a datelor medicale sau a unor informații statistice legate de sănătate. De exemplu, **dosarele medicale** ale pacienților trebuie păstrate de către unitățile medicale pentru o perioadă minimă de **10 ani** după ultimul tratament administrat.
   - Datele pentru statistici și rapoarte, care nu sunt direct legate de un pacient individual, pot fi păstrate mai mult timp, dar trebuie să fie anonimizate după un interval rezonabil, pentru a proteja confidențialitatea persoanelor vizate.
3. **Politica internă a SAJ Iasi**:
   - SAJ Iasi trebuie să stabilească, printr-o **politică internă** sau **proceduri specifice**, perioadele exacte de păstrare a datelor statistice, în funcție de tipul datelor și de necesitățile operaționale și de raportare ale serviciului.
4. **Date anonimizate sau agregate**:
   - Datele statistice anonimizate sau agregate (care nu mai pot fi atribuite unei persoane fizice) pot fi păstrate pe termen nelimitat, în scopuri de cercetare, analiză și planificare a serviciilor.

5. **Excepții**:
    - În anumite cazuri, dacă există o obligație legală de păstrare a datelor pe termen lung (de exemplu, în cazul unui audit sau al unui proces legal), aceste date pot fi păstrate pentru o perioadă mai lungă decât perioada standard prevăzută de politica internă.

Recomandări pentru compartimentul de statistică al SAJ Iasi:

- **Documentarea perioadelor de păstrare**: Compartimentul de statistică ar trebui să stabilească clar, într-o politică internă, perioadele de păstrare a datelor, în funcție de tipologia acestora și scopurile pentru care sunt prelucrate.
- **Revizuirea periodică**: Este recomandat să se revizuiască periodic necesitatea păstrării datelor și, după îndeplinirea scopurilor, să se procedeze la ștergerea sau anonimizarea acestora.
- **Păstrarea datelor anonimizate**: Dacă datele sunt necesare pentru analize statistice și nu mai pot fi atribuite unei persoane, acestea pot fi păstrate pe termen nelimitat.

În concluzie, perioada de păstrare a datelor în cadrul compartimentului de statistică al S.A.J Iași trebuie să fie stabilită în conformitate cu reglementările legale, scopurile prelucrării și politica internă a S.A.J, respectând principiile GDPR și protejând confidențialitatea pacienților, aparținătorilor și a colaboratorilor.

11. Măsuri de Securitate

În cadrul compartimentului de statistică al Serviciului de Ambulanță Județean Iași (S.A.J), măsurile de securitate pentru protejarea datelor cu caracter personal prelucrate sunt esențiale pentru a asigura confidențialitatea, integritatea și disponibilitatea acestora, în conformitate cu cerințele **Regulamentului (UE) 2016/679 (GDPR)**. Aceste măsuri sunt aplicate pentru a preveni accesul neautorizat, pierderea sau modificarea datelor, și pentru a asigura respectarea drepturilor persoanelor vizate.

Măsuri de securitate generale aplicabile în cadrul compartimentului de statisticăal S.AJ Iași:

1. **Confidențialitatea și limitarea accesului la date**
   - **Controlul accesului**: Datele cu caracter personal trebuie accesibile doar persoanelor autorizate care au nevoie de acestea pentru îndeplinirea atribuțiilor de serviciu. Se implementează **roluri și permisiuni** de acces clare în cadrul sistemelor informatice.
   - **Autentificare și autentificare dublă (2FA)**: Utilizarea unor metode de autentificare securizate, cum ar fi parole complexe și autentificarea în doi pași, pentru a preveni accesul neautorizat la datele personale.
2. **Pseudonimizarea și anonimizarea datelor**
   - **Pseudonimizarea**: Datele cu caracter personal pot fi pseudonimizate pentru a reduce riscurile de identificare a persoanelor, în cazul în care nu este necesar să se păstreze legătura directă cu persoana vizată în scopuri statistice.
   - **Anonimizarea**: Atunci când datele nu mai sunt necesare pentru scopuri specifice, acestea ar trebui să fie anonimizate, astfel încât să nu poată fi utilizate pentru a identifica o persoană fizică.
3. **Criptarea datelor**
   - **Criptarea în tranzit și în repaus**: Datele cu caracter personal trebuie criptate atât atunci când sunt transmise prin rețele (de exemplu, prin protocoale securizate precum HTTPS), cât și atunci când sunt stocate în sisteme informatice. Aceasta protejează datele împotriva accesului neautorizat în cazul în care sunt interceptate sau accesate ilegal.
   - **Criptarea fișierelor sensibile**: Dacă datele sunt stocate pe suporturi fizice (ex. USB, hard disk), criptarea acestora asigură protecția datelor în caz de pierdere sau furt al echipamentelor.

4. **Protecția fizică a echipamentelor**
    - **Măsuri de protecție fizică**: Accesul la servere, calculatoare sau alte dispozitive care stochează date sensibile trebuie să fie restricționat prin controlul accesului fizic. Acestea trebuie păstrate într-o locație securizată, cu sisteme de alarmă și supraveghere video, dacă este necesar.
    - **Distrugerea corespunzătoare a suporturilor de date**: Atunci când echipamentele de stocare a datelor nu mai sunt utilizate, trebuie să se aplice proceduri de distrugere fizică sau distrugere software a datelor pentru a preveni accesul neautorizat.
5. **Audit și monitorizare**
    - **Jurnale de audit**: Toate accesările și modificările aduse datelor trebuie să fie înregistrate în jurnale de audit pentru a putea fi verificate ulterior, în cazul unei anchete interne sau externe. Aceste jurnale trebuie să fie protejate pentru a nu fi alterate.
    - **Monitorizarea activității utilizatorilor**: Se monitorizează activitățile utilizatorilor care accesează datele pentru a detecta comportamente neobișnuite sau potențial abuzive.

În cazul S.A.J Iași, există un singur salariat în cadrul compartimentului de statistică, iar acesta are un rol crucial în implementarea corectă a **GDPR** (Regulamentul General privind Protecția Datelor) la nivelul instituției.

1. Colaborarea cu DPO-ul

- Salariatul va colabora direct cu **DPO-ul** pentru a se asigura că prelucrarea datelor cu caracter personal respectă **GDPR** și politica internă a instituției.
- În caz de necesitate, salariatul va consulta **DPO-ul** pentru clarificări legate de interpretarea reglementărilor GDPR și pentru identificarea măsurilor de protecție a datelor specifice.

2. Implementarea politicilor interne și procedurilor de protecție a datelor

- Salariatul va implementa **politicile de protecție a datelor** stabilite de instituție și va aplica procedurile de prelucrare a datelor conform cu reglementările legale.
- Va asigura aplicarea principiilor **minimizării datelor** și **transparenței** în prelucrarea datelor statistice.

3. Prelucrarea datelor pentru scopuri statistice

- Salariatul se va asigura că datele colectate și prelucrate în cadrul compartimentului de statistică sunt utilizate exclusiv în scopuri **statistice** și **anonimizate** sau **pseudonimizate** acolo unde este posibil, în conformitate cu reglementările GDPR.
- Va colabora cu DPO-ul pentru a evalua riscurile prelucrării și a efectua evaluări de impact asupra protecției datelor (DPIA) atunci când este necesar.

4. Gestionarea drepturilor persoanelor vizate

- Salariatul va facilita exercitarea drepturilor persoanelor vizate, cum ar fi **dreptul de acces, rectificare, ștergere sau portabilitate** a datelor, având ca punct de contact DPO-ul și conducerea instituției, pentru a asigura respectarea termenelor legale.
- În cazul unor solicitări din partea persoanelor vizate, salariatul va colabora cu DPO-ul pentru a răspunde prompt și corespunzător acestora.

5. Siguranța și securitatea datelor

- Salariatul va aplica măsurile de protecție a datelor stabilite de DPO și conducerea instituției, va asigura **securitatea fizică** și **tehnică** a datelor statistice.
- Va verifica dacă platformele și instrumentele utilizate pentru prelucrarea datelor respectă măsurile de securitate impuse de **DPO**.

6. Monitorizarea activităților de prelucrare

- Salariatul biroului de statistică din cadrul Serviciului de Ambulanță Județean Iași, va monitoriza în continuare activitățile de prelucrare a datelor în compartimentul de statistică și va informa DPO-ul și conducerea instituției cu privire la orice nereguli sau incidente care ar putea apărea în cadrul procesului de prelucrare.
- Va colabora cu DPO-ul pentru a evalua periodic conformitatea proceselor de prelucrare a datelor și pentru a îmbunătăți măsurile de protecție a acestora.

7. Gestionarea incidentelor de securitate

- În cazul unui incident de securitate legat de datele cu caracter personal, salariatul va informa imediat **DPO-ul** și va implementa măsurile corective în colaborare cu acesta.
- Va participa activ în procesul de **investigare** și **remediere** a incidentelor de securitate legate de datele personale din cadrul compartimentului de statistică.

8. Documentarea prelucrării datelor

- Salariatul va menține un **registru al activităților de prelucrare** a datelor, pe care îl va actualiza periodic, sub supravegherea DPO-ul, pentru a se asigura că toate activitățile de prelucrare sunt documentate corespunzător.

9. Consultarea DPO-ului în caz de îndoieli

- În cazul în care salariatul are îndoieli cu privire la conformitatea prelucrării datelor sau la implementarea unor măsuri de protecție, acesta va consulta DPO-ul pentru a asigura o abordare corectă și conformă cu legislația.

Chiar dacă există un DPO desemnat, salariatul din compartimentul de statistică va juca un rol important în implementarea și monitorizarea măsurilor de protecție a datelor la nivelul S.A.J.Iași. Responsabilitățile sale vor fi mai mult legate de **aplicarea practică a procedurilor interne**, de

colaborarea cu DPO-ul pentru evaluarea riscurilor și de **respectarea cerințelor GDPR** pentru prelucrarea datelor statistice, iar DPO-ul va asigura supravegherea globală și conformitatea instituției cu legislația privind protecția datelor.

10. Drepturile Persoanelor Vizate a căror date sunt prelucrate în cadrul biroului statistică

- **Drepturi ale angajaților**:
  - Dreptul de acces la propriile date.
  - Dreptul de rectificare și ștergere a datelor.
  - Dreptul de a solicita restricționarea prelucrării.
  - Dreptul de a depune o plângere la autoritatea de supraveghere (ANSPDCP).

Exemplu de completare a Registrului de Prelucrare a Datelor cu Caracter Personal din cadrul biroului de statistica:

Nr. crt.	Tipul activității	Scopul prelucrării	Categoria persoanelor vizate	Tipuri de date colectate	Temei legal	Durata stocării	Categorie destinatari	Unde stocăm datele?	Cine intră în contact cu datele?	Risc	Persoana responsabilă la nivel de birou
1	Colectare date statistice privind solicitările	Elaborarea rapoartelor statistice pentru analiza activității și raportarea către autorități (DSP, Ministerul Sănătății)	Pacienți	Nume, prenume, CNP, adresă, date medicale (diagnostic, tratament, detalii apel)	Art. 6(1)(c) GDPR – Obligație legală (Legea nr. 95/2006, OMS 1091/2006)	10 ani (conform legislației)	DSP, Ministerul Sănătății	Server local SAJ; Arhive fizice	Statistician birou, IT autorizat	Acces neautorizat, breșă de securitate	[Nume responsabil birou]
2	Gestionarea rapoartelor interne	Monitorizarea activității echipajelor și a resurselor utilizate în intervenții	Angajați	Nume, funcție, date privind turele, apeluri gestionate	Art. 6(1)(e) GDPR – Interes public	5 ani	Manager SAJ, autorități judiciare (la cerere)	Software intern SAJ, fișiere Excel protejate	Statistician birou	Acces intern necontrolat	[Nume responsabil birou]
3	Raportări către autorități	Transmiterea datelor statistice către autoritățile de sănătate publică	Pacienți, echipaje	Date agregate (număr cazuri, tip intervenții, localizare)	Art. 6(1)(c) GDPR – Obligație legală	10 ani	DSP, Ministerul Sănătății	Platforme de raportare DSP; Email securizat	Statistician birou	Riscuri de interceptare în timpul transmiterii	[Nume responsabil birou]
4	Gestionarea solicitărilor pentru acces la date	Răspuns la cereri din partea pacienților sau autorităților (ex.: acces la fișa intervenției)	Pacienți, autorități	Date colectate prin intermediul solicitărilor scrise	Art. 6(1)(c) GDPR – Obligație legală	Pe durata rezolvării cererii + 1 an	DSP, autorități judiciare	Dosare arhivate fizic și electronic	Statistician birou, secretariat SAJ	Pierderea sau accesul neautorizat la datele fizice	[Nume responsabil birou]

XIII. Formarea și instruirea personalului

- **Instruirea continuă a personalului**: Toți angajații și colaboratorii care manipulează datele cu caracter personal trebuie să primească instruire periodică privind securitatea datelor și politicile interne de protecție a acestora.
- **Politici interne de securitate**: SAJ Iași trebuie să dezvolte și să implementeze politici și proceduri clare privind securitatea datelor, iar personalul trebuie să fie conștient de riscurile asociate cu prelucrarea datelor și de măsurile de protecție.

Frecvența instruirilor

- Frecvență: cel puțin o dată pe an.
- Metodă: sesiuni față-în-față, e-learning sau materiale scrise.
- Evidență: registru cu semnături sau înregistrare electronică a participării.

Responsabil: DPO.

XIV.Evaluarea riscurilor și testarea măsurilor de securitate

- **Evaluări periodice ale riscurilor**: S.A.J Iași trebuie să efectueze evaluări periodice ale riscurilor legate de prelucrarea datelor, pentru a identifica vulnerabilitățile și a lua măsuri corective.
- **Testarea măsurilor de securitate**: Este recomandat ca măsurile de securitate să fie testate regulat (de exemplu, prin audituri interne și externe, teste de penetrare) pentru a verifica eficiența acestora.

XV. Gestionarea incidentelor de securitate

1. Scop

Această secțiune reglementează pașii ce trebuie urmați în cazul apariției unui incident de securitate privind datele cu caracter personal, în vederea limitării impactului, notificării conforme cu prevederile legale și restaurării datelor, asigurând astfel continuitatea activității în cadrul Serviciului de Ambulanță Județean Iași (S.A.J. Iași).

2. Definirea incidentului de securitate

Un **incident de securitate** este orice eveniment care duce sau poate duce la:

- accesarea neautorizată a datelor cu caracter personal;
- pierderea, furtul sau distrugerea accidentală/intenționată a datelor;
- modificarea neautorizată a datelor;
- compromiterea disponibilității, integrității sau confidențialității datelor.

3. Plan de răspuns la incidente de securitate

3.1 Etapele răspunsului operațional

Etapa 1: Identificarea și raportarea incidentului

- Orice angajat care observă sau suspectează un incident de securitate este obligat să îl raporteze imediat către Responsabilul cu Protecția Datelor (DPO) sau conducerea directă.
- Se va completa formularul de raportare a incidentului (Anexa X).

Etapa 2: Confirmarea și clasificarea incidentului

- DPO, împreună cu echipa IT și/sau alte persoane desemnate, va evalua incidentul pentru a stabili natura, gravitatea și impactul acestuia.
- Se clasifică nivelul de risc: scăzut, mediu sau ridicat.

Etapa 3: Măsuri de limitare a impactului

- Se vor lua măsuri tehnice și organizatorice urgente pentru a limita efectele incidentului: deconectare de la rețea, schimbarea parolelor, izolarea echipamentelor etc.

Etapa 4: Notificarea autorităților

- Dacă există un risc pentru drepturile și libertățile persoanelor fizice, DPO va notifica **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)** în termen de **cel mult 72 de ore** de la constatarea incidentului, conform art. 33 din GDPR.
- Notificarea va include:
  - natura incidentului;
  - categoriile și numărul estimativ al persoanelor vizate;
  - măsurile luate sau propuse;
  - datele de contact ale DPO-ului.

Etapa 5: Informarea persoanelor vizate

- Dacă incidentul prezintă un risc ridicat pentru drepturile și libertățile persoanelor, acestea vor fi informate **fără întârzieri nejustificate**, cu menționarea măsurilor luate pentru reducerea impactului.

Etapa 6: Documentarea incidentului

- Fiecare incident va fi înregistrat într-un **Registru al incidentelor de securitate** care va conține:

- data incidentului;
- descrierea detaliată;
- evaluarea impactului;
- măsurile luate;
- concluziile și lecțiile învățate.

4. Proceduri de recuperare și continuitate

4.1 Măsuri proactive

- Se asigură realizarea de **copii de siguranță (backup)** conform unei politici prestabilite (zilnic, săptămânal).
- Se testează periodic (trimestrial) integritatea și funcționalitatea acestor backup-uri.
- Copiile de rezervă sunt păstrate în medii sigure, accesibile doar personalului autorizat.

4.2 Restaurarea datelor

- În cazul pierderii sau compromiterii datelor, echipa IT va iniția procedura de restaurare a datelor din backup în cel mai scurt timp posibil.
- Se va urmări:
  - recuperarea completă și corectă a datelor afectate;
  - minimizarea întreruperilor în activitate;
  - validarea datelor restaurate.

4.3 Responsabilități

- **DPO**: coordonarea generală, notificări legale, comunicare cu ANSPDCP și persoanele vizate.
- **Departamentul IT**: limitarea efectelor tehnice, restaurarea datelor, raport tehnic post-incident.
- **Conducerea**: sprijin decizional și organizatoric.

5. Îmbunătățirea continuă

- După fiecare incident, se organizează o analiză internă („post-mortem") pentru a:
  - identifica cauzele rădăcină;
  - evalua eficiența răspunsului;
  - actualiza procedurile și măsurile de securitate;
  - instrui personalul implicat.

6. Anexe

- Anexa 1 – Formular de Raportare Incident de Securitate a Datelor cu Caracter Personal
- Anexa 2 – Model notificare ANSPDCP
- Anexa 3 – Model notificare către persoanele vizate
- Anexa 4 – Registrul incidentelor de securitate a datelor
- Anexa 5 - Formular consimțământ si informare privind prelucrarea datelor cu caracter personal, pentru activități educative – minori
- Anexa 6 - Formular Cerere - Exercitarea Drepturilor conform GDPR
- Anexa 7 - Cerere pentru exercitarea dreptului de opoziție asupra prelucrării datelor cu caracter personal
- Anexa 8 - Acord de Prelucrare a Datelor cu Caracter Personal conform Regulamentului GDPR
- Anexa 9 -Acord de confidențialitate
- Anexa 10 -Consmțământ prelucrarea datelor cu caracter personal
- Anexa 11– Formular de Raportare a Breșei de Securitate a Datelor cu Caracter Personal

XVI. Gestionarea Breșelor de Securitate a Datelor cu Caracter Personal

Conform articolelor **33 și 34 din Regulamentul (UE) 2016/679 (GDPR)**, Serviciul de Ambulanță Județean Iasi are obligația de a identifica, investiga și notifica eventualele încălcări ale securității datelor cu caracter personal care pot genera un risc pentru drepturile și libertățile persoanelor vizate.

1. Definirea breșei de securitate

O breșă de securitate reprezintă o încălcare a securității care duce, accidental sau ilegal, la:

- distrugerea,
- pierderea,
- modificarea,
- divulgarea neautorizată a datelor cu caracter personal sau
- accesul neautorizat la acestea.

Exemple frecvente:

- pierderea sau distrugerea fișelor medicale ale pacienților;
- trimiterea eronată a datelor către alt destinatar;
- acces neautorizat în sistemele informatice interne;
- furtul unui laptop/dispozitiv care conține date personale.

2. Procedura de detectare, notificare și documentare a breșelor de securitate (art. 33–34 GDPR)"

1. Detectarea incidentului de securitate (raport intern imediat către DPO).
2. Evaluarea impactului asupra datelor și persoanelor vizate.
3. Notificarea ANSPDCP în termen de maximum 72 de ore, conform art. 33 GDPR.
4. Informarea persoanelor vizate, dacă este cazul, conform art. 34 GDPR.
5. Documentarea completă a incidentului într-un „Registru al breșelor de securitate".

Model minim de formular pentru raportarea breșei este anexat în Anexa 11.

3. Mecanism de raportare internă

Toți angajații SAJ au obligația să informeze imediat Responsabilul cu protecția datelor (DPO) despre orice suspiciune sau incident de securitate.
Raportarea trebuie făcută **în maximum 12 ore** de la constatarea incidentului, prin:

- completarea unui formular de incident (intern),
- transmiterea unui email securizat către DPO.

4. Evaluarea breșei

După primirea sesizării, DPO are sarcina de a evalua rapid incidentul pentru a determina:

- natura și volumul datelor compromise;
- categoriile de persoane vizate;
- potențialul impact asupra acestora;
- dacă este necesară notificarea autorității;
- măsurile luate pentru remedierea situației.

5. Notificarea ANSPDCP

Dacă în urma evaluării se constată că breșa este susceptibilă să afecteze drepturile și libertățile persoanelor, SAJ va notifica **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**, în cel mult **72 de ore** de la luarea la cunoștință a breșei, conform art. 33 GDPR.

Notificarea va conține:

- descrierea naturii încălcării;
- categoriile și numărul estimat de persoane afectate;
- măsurile corective întreprinse;
- datele de contact ale DPO.

6. Informarea persoanelor vizate

Dacă breșa reprezintă un **risc ridicat** pentru drepturile și libertățile persoanelor, SAJ va informa în mod direct persoanele afectate **fără întârzieri nejustificate**, conform art. 34 GDPR.

7. Evidența breșelor

Toate incidentele, indiferent dacă au fost sau nu notificate, se vor înregistra într-un **Registru al breșelor de securitate** păstrat de DPO.
Registrul va conține:

- descrierea breșei,
- data producerii,
- data sesizării,
- măsurile corective adoptate,
- concluziile evaluării.

XVII. Evaluarea impactului asupra protecției datelor (DPIA)

- **DPIA (Data Protection Impact Assessment)**: În cazul în care prelucrarea datelor implică un risc ridicat pentru drepturile și libertățile persoanelor vizate (de exemplu, procesarea unor date sensibile în scopuri de statistică), S.A.J trebuie să efectueze o evaluare a impactului asupra protecției datelor înainte de începerea prelucrării.

Implementarea acestor măsuri este esențială pentru protejarea datelor cu caracter personal prelucrate în cadrul compartimentului de statistică al S.A.J Iași, asigurând conformitatea cu legislația în vigoare și protejarea drepturilor persoanelor vizate. Aceste măsuri ajută nu doar la prevenirea accesului neautorizat și a riscurilor de securitate, ci și la construirea unei culturi organizaționale care pune un accent puternic pe protecția datelor cu caracter personal.

XVIII. Responsabilități

Pentru implementarea corectă și completă a prezentei proceduri operaționale privind Registrul de Evidență a Datelor cu Caracter Personal, responsabilitățile se împart astfel:

1. Responsabilitățile conducerii Serviciului de Ambulanță Județean

- Asigurarea resurselor necesare pentru aplicarea procedurii și pentru protecția datelor cu caracter personal.
- Nominalizarea responsabililor pentru completarea Registrului de Evidență a Datelor cu Caracter Personal la nivel de compartimente și servicii.
- Verificarea periodică a implementării procedurii și respectării obligațiilor de către personal.

2. Responsabilitățile persoanei responsabile cu protecția datelor (DPO)

- Oferirea de consiliere și suport personalului în completarea Registrului.
- Monitorizarea respectării prevederilor GDPR și ale prezentei proceduri.
- Organizarea sesiunilor de instruire a personalului în domeniul protecției datelor cu caracter personal.
- Verificarea corectitudinii și completitudinii datelor înscrise în Registru prin audituri periodice.

- Sesizarea conducerii în cazul constatării unor nereguli privind gestionarea datelor.

3. Responsabilitățile coordonatorilor de compartimente și servicii

- Implementarea și respectarea procedurii la nivelul compartimentului/serviciului coordonat.
- Supravegherea activităților de prelucrare a datelor cu caracter personal și a completării corecte a Registrului.
- Asigurarea că personalul din subordine respectă măsurile de protecție a datelor și completează registrul conform cerințelor.
- Raportarea către conducere sau DPO a oricăror incidente de securitate privind datele cu caracter personal.

4. Responsabilitățile personalului implicat în prelucrarea datelor cu caracter personal

- Respectarea regulilor și măsurilor stabilite în această procedură.
- Completarea corectă și la timp a Registrului de Evidență a Datelor cu Caracter Personal, conform instrucțiunilor primite.
- Protejarea datelor cu caracter personal și evitarea oricăror acțiuni care ar putea compromite securitatea acestora.
- Anunțarea imediată a coordonatorului sau a DPO-ului în cazul identificării unor nereguli sau incidente de securitate.

5. Responsabilitățile biroului de statistică

- Centralizarea și raportarea datelor statistice, respectând confidențialitatea și securitatea acestora.
- Completarea registrului pentru activitățile proprii și coordonarea cu celelalte compartimente implicate.

- Colaborarea cu DPO-ul pentru a asigura conformitatea cu cerințele legale privind protecția datelor.

6. Responsabilitățile altor terți sau colaboratori

- Persoanele împuternicite sau colaboratorii implicați în prelucrarea datelor în numele Serviciului de Ambulanță Județean trebuie să respecte termenii contractuali și cerințele prezentei proceduri.
- Furnizarea informațiilor și documentației necesare pentru completarea registrului, dacă este cazul.

XIX Politica de retenție a datelor în SAJ

- În cadrul Serviciului de Ambulanță Județean Iași (S.A.J), gestionarea și păstrarea datelor se realizează în conformitate cu legislația în vigoare și cu cerințele specifice domeniului medical și administrativ. Pentru a asigura transparență, protecția datelor și conformitatea legală, s-au stabilit perioade standard de retenție a principalelor categorii de date.

Tip de date	Perioada de retenție	Bază legală / Observații
Fișe medicale pacienți	5 ani	Conform legislației medicale în vigoare
Documente HR (contracte, state de plată)	75 ani	Legea Arhivelor Naționale
Înregistrări video de supraveghere	Maximum 30 zile	Dacă nu există incident
Documente contabile	10 ani	Legea contabilității

XX. Audit și revizuire procedură

Protecția datelor cu caracter personal este un aspect fundamental pentru Serviciul de Ambulanță Județean Iași, fiind reglementată prin Regulamentul General privind Protecția Datelor (GDPR) și legislația națională aferentă. Respectarea acestor reglementări asigură drepturile persoanelor vizate și integritatea informațiilor gestionate.

Pentru a garanta conformitatea continuă cu GDPR și alte cerințe legale, se efectuează audituri interne periodice privind protecția datelor, cu o frecvență anuală. Scopul acestor audituri este de a verifica respectarea procedurilor interne, a măsurilor tehnice și organizatorice implementate, precum și de a identifica eventualele riscuri și neconformități.

Orice modificare sau actualizare a procedurii de protecție a datelor va fi supusă aprobării conducerii SAJ, responsabilitatea finală revenind directorului instituției sau persoanei delegate. Astfel, se asigură un control riguros și o adaptare continuă a politicilor la evoluția cadrului legal și a necesităților organizaționale, în conformitate cu principiile GDPR.

XXI. Încheiere

Această procedură operațională privind prelucrarea datelor cu caracter personal în cadrul Serviciului de Ambulanță Județean (SAJ) reprezintă un instrument esențial pentru asigurarea conformității cu legislația în vigoare, în special cu Regulamentul General privind Protecția Datelor (GDPR). Implementarea acestei proceduri are drept scop protejarea datelor cu caracter personal ale persoanelor vizate, respectarea drepturilor acestora și prevenirea oricăror încălcări ale securității datelor.

Toți angajații și colaboratorii SAJ IAȘI sunt obligați să cunoască și să aplice corect prevederile acestei proceduri, asigurându-se astfel că prelucrarea datelor personale se face în mod transparent, sigur și conform legii. Responsabilitatea respectării procedurii revine fiecărui angajat al instituției,

precum și persoanelor desemnate pentru gestionarea datelor, inclusiv responsabililor cu protecția datelor și persoanelor responsabile pentru securitatea informațiilor.

Este important ca, prin aplicarea acestei proceduri, SAJ IASI să demonstreze angajamentul său față de protecția datelor personale, să monitorizeze periodic respectarea reglementărilor GDPR și să adopte măsurile necesare pentru a răspunde eventualelor incidente de securitate.

Această procedură operațională va fi revizuită periodic, pentru a reflecta eventualele schimbări legislative sau organizaționale, și va fi actualizată ori de câte ori este necesar pentru a asigura conformitatea continuă cu cerințele legale și cele mai bune practici în domeniul protecției datelor personale.

În concluzie, registrul de prelucrare a datelor este un instrument vital pentru protecția datelor personale și pentru îndeplinirea obligațiilor legale ale instituției, contribuind la menținerea unui mediu sigur și conform în cadrul activităților de prelucrare a datelor cu caracter personal.

Anexa 1

Anexa 1 – Formular de Raportare Incident de Securitate a Datelor cu Caracter Personal

Serviciul de Ambulanță Județean Iași
Formular Intern de Raportare Incident GDPR

1. Informații generale

Data raportării incidentului [//_____]
Ora raportării [:]
Numele persoanei care raportează _____
Funcția _____
Departamentul / Compartimentul _____

2. Descrierea incidentului

Data și ora producerii incidentului	[//] – [:___]
Locul producerii	_____
Tipul incidentului (bifează):	☐ Acces neautorizat ☐ Pierdere date ☐ Furt/dispariție echipament ☐ Modificare neautorizată ☐ Alte situații: _____
Descriere detaliată a incidentului	*(Se va descrie cum a fost identificat incidentul, ce date au fost implicate, circumstanțele etc.)*

3. Măsuri imediate luate

Ce acțiuni s-au întreprins inițial? _____
Persoane implicate _____

4. Alte observații relevante

_____

Semnătura raportorului: _____
Data: //_____

Anexa 2

Anexa 2 – Model notificare către ANSPDCP

Către: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
Adresa: B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, București
Email: [notificari@dataprotection.ro]

Subiect: Notificare incident de securitate conform art. 33 GDPR
Notificator: Serviciul de Ambulanță Județean Iași
Cod de identificare instituțional: (CUI)

1. Descrierea incidentului

- **Data și ora descoperirii:** //_____
- **Data producerii incidentului (estimativ):** //_____
- **Tipul incidentului:**
  ☐ Acces neautorizat
  ☐ Pierdere/stergere accidentală
  ☐ Modificare neautorizată
  ☐ Alte situații: _____
- **Descrierea detaliată a incidentului:**
  [Detaliere clară a contextului, sistemelor afectate, circumstanțelor]

2. Datele afectate

- Tipuri de date personale afectate:
  ☐ Nume, prenume
  ☐ CNP
  ☐ Date medicale
  ☐ Date de contact
  ☐ Alte: _____
- Număr estimativ de persoane afectate: _____

- Categoriile de persoane vizate:
  ☐ Pacienți
  ☐ Angajați
  ☐ Terți/colaboratori
  ☐ Alte categorii: _____

3. Evaluarea riscului

- Impact potențial:
  ☐ Scăzut
  ☐ Mediu
  ☐ Ridicat
- Măsuri luate:
  - Izolarea incidentului
  - Restaurare backup
  - Notificare persoane vizate (dacă este cazul)
  - Măsuri tehnice și organizatorice adiționale

4. Date de contact DPO

- Nume: _____
- Telefon: _____
- Email: _____

Semnătură reprezentant legal: _____
Data: //_____

Anexa 3

Anexa 3 – Model notificare către persoanele vizate

[Antet SAJ Iași]

Subiect: Informare privind un incident de securitate a datelor cu caracter personal

Stimate/Stimată [nume],

Vă informăm că, în data de //_____, Serviciul de Ambulanță Județean Iași a identificat un incident de securitate care a afectat datele dumneavoastră cu caracter personal.

1. Ce s-a întâmplat?

[Scurtă descriere a incidentului, fără a dezvălui date sensibile sau interne inutile]

2. Ce tip de date au fost afectate?

[Ex: nume, prenume, CNP, date medicale]

3. Ce riscuri pot apărea?

- Acces neautorizat la date
- Posibilitate de utilizare necorespunzătoare a datelor
- Alte riscuri: _____

4. Ce măsuri am luat?

- Limitarea efectelor incidentului
- Recuperarea datelor
- Notificarea autorităților
- Monitorizare continuă a sistemelor

5. Ce puteți face dumneavoastră?

- Monitorizați activitatea conturilor personale
- Raportați orice suspiciune de utilizare neautorizată
- Pentru suport suplimentar, ne puteți contacta:

Responsabil cu protecția datelor (DPO):
Nume: _____
Email: _____
Telefon: _____

Ne cerem scuze pentru inconvenientul creat și vă asigurăm că am luat toate măsurile necesare pentru a preveni astfel de situații în viitor.

Cu stimă,
Conducerea SAJ Iași
Data: //_____

Anexa 4 – Registrul incidentelor de securitate a datelor

Nr. crt	Data incidentului	Descriere incident	Tip date afectate	Nr. persoane afectate	Data notificării ANSPDCP	Data notificării persoanelor	Măsuri luate	Finalizare/Status
1	dd/mm/yyyy	[ex: acces neautorizat sistem medical]	Date medicale, CNP				Ex.Restaurare backup, audit IT	Finalizat

!! Registrul se păstrează de către DPO și se actualizează după fiecare incident confirmat.

Anexa 5

FORMULAR DE CONSIMȚĂMÂNT PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL ȘI INFORMAREA PRIVIND SUPRAVEGHEREA AUDIO-VIDEO PENTRU MINORII CU VÂRSTA SUB 16 ANI

Serviciul de Ambulanță Județean Iași, cu sediul în Bulevardul Primăverii nr.74, CUI 7604489, reprezentat prin Manager General ....., email office@ambulantaiasi.ro, am aprobat solicitarea primită în data de .....

Eveniment: .....

Subsemnatul/a, _____, în calitate de **părinte/tutore legal** al minorului/minorei _____, născut/ă la data de _____, elev/ă la _____, declar următoarele:

1. Consimțământ pentru prelucrarea datelor cu caracter personal

Prin prezenta, îmi exprim acordul ca **Serviciul de Ambulanță Județean Iași (SAJ Iași)** să prelucreze datele cu caracter personal ale copilului meu, în scopul organizării și desfășurării activităților educaționale din cadrul evenimentului .....

Datele prelucrate pot include:

- Nume și prenume al minorului;
- Unitate de învățământ;
- Imaginea și vocea în cazul realizării de fotografii/filmări în scop strict educativ și de promovare a evenimentului.

Datele vor fi utilizate **exclusiv pentru scopurile legate de organizarea evenimentului** și nu vor fi transmise către terți fără consimțământul explicit, cu excepția cazurilor prevăzute de lege.

2. Informare privind existența sistemului de supraveghere audio-video

Am luat la cunoștință că, în cadrul SAJ Iași, există un **sistem de supraveghere audio-video** instalat în scopul asigurării securității persoanelor și a bunurilor. Imaginile sunt prelucrate în conformitate cu legislația în vigoare privind protecția datelor cu caracter personal.

3. Drepturile părintelui/tutorelui legal și ale minorului

Conform **Regulamentului (UE) 2016/679 (GDPR)**, am fost informat/ă că beneficiez de următoarele drepturi:

- Dreptul de acces la datele prelucrate;
- Dreptul la rectificarea sau ștergerea datelor;
- Dreptul de a restricționa prelucrarea datelor;
- Dreptul de a depune o plângere la **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.**

4. Declarație finală

Prin semnătura de mai jos, confirm că:

- Am citit și am înțeles conținutul acestui formular;
- Sunt de acord cu prelucrarea datelor cu caracter personal menționate mai sus;
- Am fost informat/ă cu privire la supravegherea audio-video din cadrul SAJ Iași.

Data: _____
Semnătura părinte/tutore legal: _____
Nume și prenume (în clar): _____

Notă: Acest consimțământ poate fi retras oricând, printr-o cerere scrisă adresată S.A.J. Iași.

Anexa 6

Formular Cerere - Exercitarea Drepturilor conform GDPR

Conform Regulamentului (UE) 2016/679 (GDPR), persoanele vizate au dreptul de a solicita accesul, rectificarea, ștergerea, restricționarea sau portabilitatea datelor, precum și de a se opune prelucrării acestora. Completați formularul de mai jos pentru a vă exercita unul dintre aceste drepturi.

I. Datele de identificare ale persoanei vizate

Nume și prenume: _____

CNP _____

Adresa de domiciliu: _____

Număr de telefon: _____

Adresă de e-mail: _____

II. Dreptul pe care doriți să îl exercitați

Bifați opțiunea corespunzătoare:

☐ Dreptul de acces la datele cu caracter personal

☐ Dreptul la rectificarea datelor

☐ Dreptul la ștergerea datelor („dreptul de a fi uitat")

☐ Dreptul la restricționarea prelucrării

☐ Dreptul la portabilitatea datelor

☐ Dreptul la opoziție

☐ Altul: _____

III. Detalii privind cererea

Vă rugăm să descrieți în mod clar solicitarea dumneavoastră și, dacă este cazul, datele vizate:

_____

IV. Confirmare

Declar că această cerere este întocmită în nume propriu sau în calitate de reprezentant legal al persoanei vizate și că informațiile furnizate sunt corecte.

Semnătura: _____ Data: _____

Notă: SAJ Iasi prelucrează aceste date exclusiv în scopul soluționării cererii dumneavoastră, în conformitate cu art. 12-23 din GDPR.

Anexa 7

CERERE

pentru exercitarea dreptului de opoziție asupra prelucrării datelor cu caracter personal

În conformitate cu prevederile **art. 21** din **Regulamentul (UE) nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date** (Regulamentul General privind Protecția Datelor - RGPD), prin prezenta îmi exercit dreptul la opoziție asupra prelucrării datelor mele cu caracter personal care sunt prelucrate în temeiul îndeplinirii unei sarcini care servește unui interes public sau în scopul intereselor legitime urmărite de operator de către **Serviciul de Ambulanță Județean Iași.**

În vederea obținerii unui răspuns, vă pun la dispoziție următoarele informații:

1. DATE PRIVIND PERSOANA CARE SOLICITĂ INFORMAȚII

Subsemnatul/a.....CNP.....,

act de identitate seria ..... nr....., cu domiciliul/reşedinţa în localitatea ....., str. ....., nr....., bl. ....., sc. ....., ap.....judeţ/sector....., telefon ....., adresa de e-mail ..... .

În calitate de (*vă rugăm să bifați căsuțele corespunzătoare calității dvs.*):

o **persoană vizată** (Termenul "persoană vizată" este folosit pentru a desemna persoana fizică despre care se solicită informații prin prezenta cerere)

o **reprezentant legal al persoanei vizate**, conform documentului/actului atașat la prezenta cerere.

2. DATE PRIVIND PERSOANA VIZATĂ (se completează în situația în care persoana menționată la pct. 1 are calitate de reprezentant legal)

Subsemnatul/a.....CNP....., act de identitate seria ..... nr....., cu domiciliul/reşedinţa în localitatea

....., str.
.....,nr.....,bl.....,sc.....,
ap.....județ/sector....., telefon ....., adresa de e-mail ..... .

3. PRECIZAȚI DATELE ASUPRA CĂRORA DORIȚI SĂ VĂ EXERCITAȚI ACEST DREPT

Vă rugăm să descrieți informațiile asupra cărora va exercitați acest drept și să furnizați informații suficiente care ar putea să ne fie de ajutor în identificarea acestora. De asemenea, vă rugăm să precizați motivul/motivele care stau la baza solicitării dvs. și să atașați prezentei documente în susținere.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Doresc ca răspunsul să îmi fie comunicat:

□ În format electronic, la următoarea adresă de e-mail:

.....

□ Prin poștă, la următoarea adresă (se menționează adresa de corespondență)

4. DECLARAȚIE

Subsemnatul/a ....., confirm faptul că informațiile furnizate de mine prin această cerere sunt reale și corecte, iar datele enumerate mai sus sunt singurele la care solicit accesul. Am fost informat că datele cu caracter personal furnizate prin prezenta cerere vor fi utilizate numai în scopul soluționării cererii mele de acces la date cu caracter personal.

Am luat la cunoștință prevederile **art. 326 – Falsul în declarații** și **art.327 – Falsul privind identitatea** din Codul Penal și declar pe proprie răspundere că nu am avut și nu am folosit alte nume și date în afara celor înscrise/atașate în/la prezenta cerere.

Am înțeles că operatorul de date cu caracter personal trebuie să confirme identitatea mea/a persoanei vizate și că, în scopul clarificării datelor personale corespunzătoare, ar putea fi necesar să furnizez ulterior și alte informații necesare soluționării prezentei cereri.

Am înțeles că termenul de răspuns la prezenta cerere se va calcula din momentul în care vor fi îndeplinite condițiile de mai sus. Am luat la cunoștință faptul că lipsa răspunsurilor exacte la toate întrebările din formular sau necompletarea corectă a acestora face imposibilă obținerea informațiilor solicitate.

Față de cele de mai sus, vă rog să dispuneți măsurile legale pentru a primi, în termenul legal de 30 de zile, informațiile solicitate în baza Regulamentului (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

Atașez prezentei cereri următoarele documente, în copie certificate ograf cu originalul:

.....
.....
.....
.....

Anexa 8

Acord de Prelucrare a Datelor cu Caracter Personal conform Regulamentului (UE) 2016/679 (GDPR). Acesta este potrivit pentru relația dintre un operator (ex. SAJ Iași) și un împuternicit

ACORD DE PRELUCRARE A DATELOR CU CARACTER PERSONAL
Nr. ____ / Data: //_____
Încheiat între:
1. Operatorul
Denumire: Serviciul de Ambulanță Județean Iași
Sediu: [adresă completă]
CUI: [cod fiscal]
Reprezentat legal prin: [nume, funcție]
Telefon: _____
Email: _____
– denumit în continuare **Operatorul** –
și
2. Împuternicitul
Denumire: [ ]
Sediu: [adresă completă]
CUI: _____
Nr. înreg. ORC: _____
Reprezentat legal prin: [nume, funcție]
Telefon: _____
Email: _____
– denumit în continuare **Împuternicitul** –

Art. 1 – Obiectul acordului
Prezentul acord reglementează modul în care Împuternicitul va prelucra datele cu caracter personal în numele Operatorului, în conformitate cu **art. 28 din Regulamentul (UE) 2016/679 (GDPR).**

Art. 2 – Scopul și durata prelucrării
Scopul: [ex: prestarea serviciilor de mentenanță IT / arhivare documente / salarizare / audit etc.]
Durata: Pe durata contractului principal nr. ____ din data ____ și până la încetarea obligațiilor contractuale, inclusiv perioada de arhivare, conform legislației aplicabile.

Art. 3 – Categoriile de date prelucrate
Împuternicitul poate prelucra următoarele categorii de date, în funcție de obiectul contractului:
- Nume, prenume
- CNP
- Adresă
- Date de contact (telefon, e-mail)

- Date de identificare profesională
- Date medicale (dacă este cazul)
- Alte date relevante pentru scopul prelucrării

Art. 4 – Categorii de persoane vizate
- Angajați ai Operatorului
- Pacienți / beneficiari ai serviciilor SAJ
- Colaboratori / furnizori / terți

Art. 5 – Obligațiile Împuternicitului
Împuternicitul se angajează:
1. Să prelucreze datele **doar pe baza instrucțiunilor documentate** ale Operatorului.
2. Să asigure măsuri tehnice și organizatorice adecvate pentru protecția datelor.
3. Să nu transmită datele către alți terți sau subîmputerniciți fără aprobarea prealabilă scrisă a Operatorului.
4. Să asigure confidențialitatea datelor și să instruiască personalul implicat.
5. Să sprijine Operatorul în îndeplinirea obligațiilor privind drepturile persoanelor vizate (acces, rectificare, ștergere, opoziție, portabilitate etc.).
6. Să notifice Operatorul **fără întârziere (maxim 24h)** în cazul unui incident de securitate.
7. Să permită audituri și inspecții din partea Operatorului sau autorităților competente.
8. Să șteargă sau returneze toate datele la finalul contractului, conform instrucțiunilor Operatorului.

Art. 6 – Subîmputerniciți
Împuternicitul **nu va subcontracta** activitățile de prelucrare fără acordul prealabil scris al Operatorului. În cazul aprobării, va încheia un acord cu subîmputernicitul în aceleași condiții ca prezentul document.

Art. 7 – Securitatea prelucrării
Împuternicitul trebuie să aplice măsuri conforme cu art. 32 GDPR, inclusiv:
- Controlul accesului logic
- Autentificare și parole sigure
- Backup și restaurare
- Monitorizare și jurnalizare activități
- Protecția echipamentelor și a comunicațiilor

Art. 8 – Răspundere
Împuternicitul răspunde pentru orice prejudiciu cauzat de neîndeplinirea obligațiilor legale sau contractuale privind prelucrarea datelor. Operatorul poate solicita daune-interese.

Art. 9 – Încetare
Acordul încetează odată cu contractul principal, cu respectarea obligației de returnare sau ștergere a datelor. Obligațiile de confidențialitate rămân în vigoare și după încetare.

Art. 10 – Dispoziții finale
Acest acord:

- Este parte integrantă a contractului principal nr. ____;
- Se completează cu legislația în vigoare privind protecția datelor;
- Se încheie în două exemplare originale, câte unul pentru fiecare parte.

ANEXA 9

ACORD DE CONFIDENȚIALITATE

Nr. ____ / Data: //_____

Încheiat între:

Serviciul de Ambulanță Județean Iași

Sediu: [adresă completă]
Reprezentat legal prin: [nume, funcție]

– denumit în continuare „**Angajatorul**" –

și

Domnul/Dna [Nume și Prenume angajat]

CNP: _____
Funcția: _____

– denumit în continuare „**Angajatul**" –

Art. 1 – Obiectul acordului

Angajatul se angajează să păstreze **confidențialitatea** tuturor informațiilor, datelor cu caracter personal și a oricăror alte date sensibile la care are acces în exercitarea atribuțiilor sale în cadrul SAJ Iași.

Art. 2 – Obligațiile Angajatului

Angajatul se obligă:

1. Să nu divulge, comunice, distribuie sau folosească în alte scopuri decât cele legate strict de activitatea sa în cadrul SAJ Iași, orice informație confidențială privind datele personale ale pacienților, colegilor sau alte date sensibile.
2. Să respecte toate procedurile interne privind protecția datelor și securitatea informațiilor.

3. Să nu copieze, reproducă sau transmită informațiile confidențiale către terți, fără acordul expres scris al Angajatorului.
4. Să raporteze imediat orice incident de securitate sau posibile breșe de confidențialitate către responsabilul cu protecția datelor (DPO).
5. Să respecte interdicția de a utiliza datele sau informațiile confidențiale după încetarea raportului contractual cu Angajatorul.

Art. 3 – Durata acordului

Prezenta obligație de confidențialitate este valabilă pe toată durata raportului de muncă și continuă să producă efecte și după încetarea acestuia, fără limită de timp.

Art. 4 – Sancțiuni

Nerespectarea prezentului acord constituie abatere disciplinară și poate atrage răspunderea civilă, contravențională sau penală conform legislației în vigoare.

Art. 5 – Dispoziții finale

Prezentul acord face parte integrantă din documentația internă a SAJ Iași privind protecția datelor cu caracter personal.

Anexa 10

CONSIMȚĂMÂNT PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL

Subsemnatul/Subsemnata,
Nume și prenume: _____
CNP: _____
Domiciliu/reședință: _____
Telefon: _____
E-mail: _____

Declar că am fost informat(ă), în conformitate cu Regulamentul (UE) 2016/679 („GDPR") și Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR, cu privire la următoarele aspecte referitoare la prelucrarea datelor mele cu caracter personal:

1. Operatorul datelor

Serviciul de Ambulanță Județean Iași
Sediu: [adresă completă]
Telefon: [nr. telefon]
Email: [email contact]

2. Scopul prelucrării datelor

Prelucrarea datelor personale are ca scop:

- [exemplu: furnizarea serviciilor medicale de urgență, gestionarea programărilor, comunicări interne/externe, derularea procedurilor administrative etc.]

3. Categorii de date prelucrate

- Date identificative (nume, prenume, CNP, date de contact)
- Date medicale, dacă este cazul
- Alte date relevante pentru scopul prelucrării

4. Temelul legal al prelucrării

Prelucrarea datelor personale se bazează pe:

- Consimțământul exprimat liber, specific, informat și neechivoc, conform art. 6 alin. (1) lit. a) din Regulamentul (UE) 2016/679;
- Respectiv alte temeiuri legale aplicabile, după caz (ex: art. 9 GDPR pentru date sensibile, obligații legale ale operatorului etc.).

5. Drepturile persoanei vizate

În conformitate cu art. 15-22 din GDPR, am dreptul de a:

- Accesa datele mele personale;
- Rectifica datele inexacte sau incomplete;
- Șterge datele în anumite condiții;
- Restricționa prelucrarea;
- Opoziție la prelucrare;
- Portabilitatea datelor;
- Retrage consimțământul în orice moment fără a afecta legalitatea prelucrării efectuate anterior retragerii.

6. Durata prelucrării

Datele vor fi păstrate pentru perioada necesară îndeplinirii scopurilor prevăzute sau conform obligațiilor legale aplicabile.

7. Destinatarii datelor

Datele mele personale pot fi comunicate numai:

- Persoanelor autorizate în cadrul SAJ Iași;
- Autorităților și instituțiilor prevăzute de lege (DSP, ANSPDCP etc.), dacă este cazul;
- Împuterniciților care prelucrează date în numele SAJ Iași, conform acordurilor de prelucrare.

8. Dreptul de a depune plângere

În cazul în care consider că prelucrarea datelor mele încalcă dispozițiile GDPR, pot depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

9. Consimțământul

Prin prezenta, **îmi exprim liber, specific, informat și neechivoc consimțământul** pentru prelucrarea datelor mele cu caracter personal, în condițiile descrise mai sus.

Data: //_____

Semnătura: _____

Anexa 12 – Formular de Raportare a Breșei de Securitate a Datelor cu Caracter Personal

Acest formular se completează imediat după detectarea unei breșe de securitate a datelor cu caracter personal și se transmite către Responsabilul cu Protecția Datelor (DPO). Completarea corectă și completă a acestui document este esențială pentru respectarea obligațiilor legale prevăzute în art. 33 și 34 din GDPR.

1. Data și ora detectării incidentului	
2. Persoana care raportează (nume, funcție, compartiment)	
3. Descrierea detaliată a incidentului	
4. Tipul de date afectate (ex. date de sănătate, date financiare)	
5. Numărul aproximativ de persoane vizate afectate	
6. Cauza incidentului (dacă este cunoscută)	
7. Măsuri imediate luate pentru limitarea impactului	
8. Evaluarea impactului asupra drepturilor și libertăților persoanelor vizate	
9. Notificarea către ANSPDCP (da/nu, data și ora)	
10. Informarea persoanelor vizate (da/nu, data și ora)	
11. Nume și semnătura persoanei responsabile de completare	