

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

SPITAL DE PSIHIATRIE ȘI PENTRU
MASURI DE SIGURANȚĂ JEBEL
JUDEȚUL TIMIȘ
Nr. 1829 25.02.2026
Cons.jur.Olaru Marius Ciprian

PROCEDURA DE SISTEM
Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL

Cod: PS.SPMS.CM.21

Ediția	Revizia	Data
I	-	25.02.2026
II	-	
III	-	

1. Lista responsabililor cu elaborarea, verificarea, avizarea 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
	I	2	3	4	
1.	Avizat	Olaru Marius Ciprian	Presedinte CM	25.02.2026	
2.	Verificat pentru conformitate	Petrus Cristina	Ref.CMCSS	24.02.2026	
3.	Elaborat	DAF Consulting & Management	DPO	23.02.2026	

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

2. Cuprins

Numărul componentei în cadrul procedurii	Denumirea componentei din cadrul procedurii	Pagina
1.	Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii	1
2.	Cuprins	2
3.	Scopul procedurii documentate	2
4.	Domeniul de aplicare a procedurii	2
5.	Documente de referință (reglementări) aplicabile activității procedurale	3
6.	Definiții și abrevieri	4
7.	Descrierea procedurii	5
8.	Responsabilități în derularea activității procedurale	
9.	Formular de evidență a modificărilor procedurii	
10.	Formular de analiză a procedurii	
11.	Formular de difuzare a procedurii	
12.	Diagramă de proces	

3. Scopul procedurii

1. Prezenta procedură reglementează modul de acces, prelucrarea și protejarea datelor personale ale pacienților, salariaților/potențialilor salariați și a oricăror terțe persoane care intră în contact cu SPMS JEBEL.
2. Scopul acestei proceduri este de a garanta și proteja drepturile și libertățile fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal în conformitate cu prevederile Regulamentului (UE) 2016/679.
3. Stabilește modul de realizare a activităților de prelucrare a datelor cu caracter personal având în vedere protejarea acestora, compartimentele și persoanele implicate.
4. Dă asigurări cu privire la existența documentației adecvate derulării proceselor din spital în condiții de asigurare a prelucrării și protecției datelor cu caracter personal în conformitate cu legislația specifică în vigoare.
5. **Prezenta PS previne și / sau tratează următoarele riscuri:**
 - a) Prelucrarea neautorizată (nelegitimă) a datelor cu caracter personal prelucrate de către spital;
 - b) Libera circulație a datelor cu caracter personal prelucrate de către spital;
 - c) Lipsa asigurării proprietății datelor cu caracter personal prelucrate de către spital, în raport cu terții colaboratori.

4. Domeniul de aplicare a procedurii documentate

1. **Precizarea (definirea) activității la care se referă procedura documentată, cu delimitarea explicită a activității procedurate în cadrul portofoliului de activități desfășurate de entitatea publică:**

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1 Revizia: 0 Exemplar nr.1
---	--	--

Prin procedurarea activităților se creează mediul optim pentru realizarea misiunii și îndeplinirea obiectivelor spitalului, pentru prelucrarea și protecția datelor cu caracter personal și contribuie la evaluarea rezultatelor obținute și stabilirea măsurilor necesare creșterii calității serviciilor acordate în unitate.

2. Precizarea compartimentelor în care se implementează procedura (furnizoare de date/beneficiare

de rezultate ale activității procedurate și/sau implicate direct în activitatea procedurată) :

Prezenta PS se aplică în toate structurile unității de către toate categoriile de personal (medici, asistenți medicali, registratori medicali, infirmieri etc) care au atribuții privind accesul și/sau prelucrarea de date cu caracter personal, efectuate, în tot sau în parte, prin mijloace automate, precum și prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să fie incluse într-un asemenea sistem.

5. Documente de referință (reglementări) aplicabile activității procedurale

5.1 Reglementări internaționale

- Standardul ISO: SR EN ISO 9001:2015 – Sisteme de management al calității;
- Standardul ISO: SR EN 15224:2017 – Servicii de îngrijire a sănătății;
- Regulamentul nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), emis de Parlamentul European și Consiliul Uniunii Europene.

5.2 Legislație primară

- Legea nr. 95/2006 privind reforma în domeniul sănătății, cu modificările și completările ulterioare;
- Legea Arhivelor Naționale nr. 16 / 1996, republicată în aprilie 2014, cu modificările și completările ulterioare;
- Legea nr. 185/2017 privind asigurarea calității în sistemul de sănătate, cu modificările și completările ulterioare;
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările și completările ulterioare;
- Legea nr.102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, actualizată;
- Legea nr.129/2018 pentru modificarea și completarea Legii nr.102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr.677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Legea nr.46/2003, privind drepturile pacientului, cu modificările și completările ulterioare;
- Legea nr. 487/2002 a sănătății mintale și a protecției persoanelor cu tulburări psihice, cu modificările și completările ulterioare.

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

- i) Legea nr. 53/2003 – Codul muncii, cu modificările și completările ulterioare;
- j) Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare.
- k) Legea nr. 487/2002 a sănătății mintale și a protecției persoanelor cu tulburări psihice.

5.3 Legislația secundară

- a) Ordinul SGG nr. 600/2018 pentru aprobarea Codului controlului intern managerial al entităților publice, cu modificările și completările ulterioare;
- b) Ordinul Ministerului Sănătății nr. 446/2017 pentru aprobarea Standardelor, Procedurii și metodologiei de evaluare și acreditare a spitalelor, cu modificările și completările ulterioare;
- c) Ordinul Ministerului Sănătății Publice și al Casei Naționale de Asigurări de Sănătate nr. 1782/2006 privind înregistrarea și raportarea statistică a pacienților care primesc servicii medicale în regim de spitalizare continuă și spitalizare de zi.
- d) Ordinul MS nr. 488/2016 pentru aprobarea Normelor de aplicare a Legii sănătății mintale și a protecției persoanelor cu tulburări psihice nr. 487/2002.

5.4 Alte documente, inclusiv reglementări interne ale spitalului

- a) Regulamentul de organizare și funcționare al SPMS JEBEL;
- b) Regulamentul Intern al SPMS JEBEL;
- c) Regulamentul de organizare și funcționare al Comisiei de monitorizare a SCIM aprobat la nivelul spitalului;
- d) Fișele de post ale personalului contractual.

6. Definiții și abrevieri

6.1. Definiții ale termenilor

Cea mai mare parte a definițiilor termenilor prezentați mai jos se regăsesc în Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE) - (General Data Protection Regulation - GDPR)

Nr crt	Termenul	Definiția și/sau (dacă este cazul) actul care definește termenul
0	01	02

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

1.	Date cu caracter personal	Orice informație referitoare la o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
2	Prelucrarea datelor cu caracter personal	Orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea acestor date.
3	Consimțământul	Acordul neviciat al persoanei vizate de a-i fi prelucrate datele cu caracter personal, care trebuie să fie întotdeauna expres și neechivoc.
4	Date privind sănătatea	Date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia
5	Împuternicit/ Persoana împuternicită de către operator	O persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care prelucrează date cu caracter personal în numele operatorului.
6	Sistem de evidență datelor cu caracter personal	Orice structură organizată de date cu caracter personal, accesibilă potrivit unor criterii determinate, indiferent dacă această structură este organizată în mod centralizat ori descentralizat sau este repartizată după criterii funcționale ori geografice.
7	Terț	Orice persoană fizică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, alta decât persoana vizată, operatorul ori persoana împuternicită sau persoanele care, sub autoritatea directă a operatorului sau a persoanei împuternicite, sunt autorizate să prelucreze date.
8	Destinatar	Orice persoană fizică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, căreia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu terț. Autoritățile publice cărora li se comunică date în cadrul unei competențe speciale de anchetă nu sunt considerate destinatari.

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL		Ediția: 1
			Revizia: 0
			Exemplar nr.1

9	Persoana vizată	Persoana fizică ale cărei date cu caracter personal sunt prelucrate.
10	Date biometrice	Date cu caracter personal care rezultă în urma unor tehnici de prelucrar specifice referitoare la caracteristicile fizice, fiziologice sau comportamental ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice
11	Stocarea	Păstrarea pe orice fel de suport a datelor cu caracter personal prelucrate.
12	Datele cu caracter personal sensibile	Date cu caracter personal care dezvăluie originea rasială sau etnică, opiniil politice, confesiunea religioasă sau convingerile filozofice sau apartenența l sindicate și prelucrarea de date genetice, de date biometrice pentru identificare unică a unei persoane fizice, de date privind sănătatea sau de date privind viaț sexuală sau orientarea sexuală ale unei persoane fizice.
13	Date privind sănătatea	Date cu caracter personal legate de sănătatea fizică sau mentală a unei persoan fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia.
14	Pseudonimizare	Definește prelucrarea datelor cu caracter personal într-un asemenea mod încé acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliz informații suplimentare, cu condiția ca aceste informații suplimentare să fi stocate separat și să facă obiectul unor măsuri de natură tehnică ș organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile
15	Date genetice	Datele cu caracter personal referitoare la caracteristicile genetice moștenite sa dobândite ale unei persoane fizice, care oferă informații unice privind fiziologi sau sănătatea persoanei respective și care rezultă în special în urma unei analiz a unei mostre de material biologic recoltate de la persoana în cauză.

6.2. Abrevieri ale termenilor

Nr. crt.	Abreviere a	Termenul abreviat
0	01	02
1.	ANSPDCP	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
2.	SPMS JEBEL	Spitalul de Psihiatrie si pentru Masuri de Siguranta Jebel
3.	PD	Procedură documentată
4.	PS	Procedură de sistem
5.	SGG	Secretariatul General al Guvernului

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL		Ediția: 1
			Revizia: 0
			Exemplar nr.1

6.	MS	Ministerul Sănătății
7.	OG	Ordonanță de Guvern
8.	ISO	Organizația Internațională de Standardizare
9.	CM-SCIM	Comisia de monitorizare a sistemului de control intern managerial
10.	ST	Secretariatul tehnic al Comisiei de monitorizare
11.	SCIM	Sistemul de control intern managerial
12.	SMCSS	Serviciul Managementul Calității Serviciilor de Sănătate
13.	RUNOS	Serviciul Resurse Umane, Normare, Organizare și Salarizare
14.	FOCG	Foaie de observație clinică generală
15.	FSZ	Foaie spitalizare zi
16.	DPO	Responsabil cu protecția datelor cu caracter personal

7. Descrierea procedurii documentate

1. Generalități

- Prezenta procedură reglementează modul de acces, prelucrarea și protejarea datelor personale ale pacienților, salariaților și a oricăror terțe persoane care intră în contact cu SPMS JEBEL și stabilește măsuri tehnice și organizatorice pentru îndeplinirea obligațiilor referitoare la securitatea și controlul sistemelor informatice și a întregului sistem informațional, în vederea asigurării confidențialității datelor și informațiilor precum și pentru păstrarea în siguranță a acestora, în cadrul activității curente executate de către angajații spitalului. Prin cerințe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri și politici de securitate prin care să se asigure nivelul minim de securitate ce respectă prevederile Regulamentului (UE) 2016/679 și a legislației naționale în vigoare.
- Spitalul adoptată măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat; în acest sens la nivelul spitalului este desemnat un responsabil cu protecția datelor (DPO) și sunt implementate măsuri de stocare în siguranță a informațiilor colectate.
- Pentru îndeplinirea prevederilor legale aferente și în vederea satisfacerii cerințelor păstrării în siguranță a datelor și informațiilor stocate în mediul virtual, la nivelul spitalului sunt elaborate și implementate măsuri organizatorice și tehnice orientate pe anumite direcții de acțiune precum: Identificarea și autentificarea utilizatorului, tipul de acces, execuția copiilor de siguranță, computerele și terminalele de acces, fișierele de acces și instruirea personalului.
- Pentru îndeplinirea prevederilor legale aferente și în vederea satisfacerii cerințelor păstrării în siguranță a datelor și informațiilor stocate în format fizic, la nivelul spitalului sunt elaborate și implementate măsuri organizatorice și tehnice orientate spre accesul controlat la acestea (documentele sunt păstrate în arhiva temporară sau în cea definitivă în condiții de siguranță astfel încât acestea să fie, pe de-o parte accesibile doar personalului autorizat, iar pe de altă parte protejate de distrugeri cauzate de incendii, inundații etc).

2. Etapele procedurii și responsabilitii de proces

2.1 Etapele procedurii

- Identificarea categoriilor de date cu caracter personal prelucrate de către SPMS JEBEL
- Prelucrarea datelor cu caracter personal
- Înregistrarea datelor

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

- D. Accesul dosarului medical personal
- E. Accesul la datele cu caracter personal ale angajaților
- F. Măsurile tehnice de asigurare a securității prelucrării datelor cu caracter personal
- G. Instruirea personalului
- H. Vulnerabilități privind securitatea prelucrării datelor cu caracter personal
- I. Responsabilul cu protecția datelor (DPO)
- J. Relația cu ANSPDCP
- K. Notificarea încălcării securității datelor cu caracter personal

2.2. Modul de lucru și responsabilii de proces

A. Identificarea categoriilor de date cu caracter personal prelucrate de către SPMS JEBEL

- I. În vederea respectării obligației de a ține evidența tuturor activităților de prelucrare a datelor cu caracter personal, DPO-ul din cadrul SPMS JEBEL întocmește și păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea spitalului (Registrul general de evidență a activităților de prelucrare a datelor – **Anexa 1**).

Respectiva evidență cuprinde următoarele informații:

- a) denumirea completă a instituției și datele de contact și, după caz, ale operatorului asociat, ale reprezentantului spitalului și ale responsabilului cu protecția datelor;
- b) scopurile prelucrării;
- c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională; sunt realizate numai în cazurile în care transferurile sunt necesare pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate, în condițiile în care există o documentație care dovedește existența unor garanții adecvate;
- f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate implementate.

- II. Registrul este completat de către conducătorii departamentelor/ compartimentelor și se actualizează ori de câte ori intervin modificări cu privire la natura activităților desfășurate, structurii organizatorice, datele prelucrate, categoriile vizate, introducerea unor noi măsuri de securitate etc. Conducătorul structurii este responsabil de corectitudinea și completitudinea informațiilor furnizate prin acest registru. Registrul completat se păstrează atât în format electronic și în format fizic de către fiecare șef/coordonator de structură la locul de muncă și de către DPO.

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	Ediția: 1	
	Revizia: 0	
	Exemplar nr.1	

PROCEDURĂ DE SISTEM

Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL

III. Registrul general de evidență a activităților de prelucrare înregistrează date cu caracter personal ale următoarelor categorii de persoane fizice:

- a) Pacienți, aparținători, însoțitori, reprezentanți legali ai acestora, alți membri ai familiei;
- b) Personal medical, personal sanitar, personal medical auxiliar, personal administrativ, vizitatori,

orice persoană care intră în incinta spitalului;

- c) Terțe persoane care intră în contact cu SPMS JEBEL.

IV. În vederea oferirii serviciilor medicale, SPMS JEBEL colectează și prelucrează următoarele categorii de date cu caracter personal ale angajaților, pacienților, aparținătorilor și/sau reprezentanților legali/convenționali:

- a) Date de identificare : nume și prenume, contact, data nașterii, CNP, adresă, naționalitate, copii după acte de identitate etc.;
- b) Date de contact: adresă, adresă e-mail, telefon, telefon contact urgență/aparținători, etc.;
- c) Date despre sănătate : CID, numărul cardului de asigurat, istoricul și detaliile vaccinărilor, detalii legate de medicație, alergiile, starea prezentă și trecută privind afecțiunile medicale și chirurgicale, datele genetice, rezultatele investigațiilor de laborator și ale celor imagistice, ECG-uri, ecografii , tratamentul prescris și/sau administrat, medicul care a efectuat consultul, date privind recomandări medicale, consultații, eliberare rețete, concedii medicale, scrisoare medicala, bilet de externare, bilet de trimitere, bilet de internare, programare, datele de contact ale aparținătorilor și și ale altor medici care au consultat pacientul, împreună cu toate celelalte informații necesare acordării îngrijirilor medicale.

B. Prelucrarea datelor cu caracter personal

- I. La nivelul spitalului prelucrarea datelor cu caracter personal este realizată în vederea protejării intereselor vitale ale pacienților și cu scopul de a îndeplini una sau mai multe obligații legale ce îi revin spitalului.
- II. La nivelul spitalului este *interzisă* prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice, cu *excepția* cazului în care prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, caz în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia.
- III. La momentul colectării datelor cu caracter personal, la internare, pacienții SPMS JEBEL sunt informați de către asistentul/registratorul medical cu privire la prelucrarea datelor cu caracter personal, prin "Informarea pacienților privind prelucrarea datelor cu caracter personal" (**Anexa 2**). Pacienții sunt informați în baza documentului de informare generală pacienți privind prelucrarea datelor cu caracter personal, cu privire la:
 - a) Identitatea operatorului de date și a reprezentantului acestuia, dacă este cazul;
 - b) Scopul în care se face prelucrarea datelor;
 - c) Informații suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie și consecințele refuzului de a le furniza;

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

existența drepturilor de acces , de intervenție asupra datelor și de opoziție , precum și condițiile în care pot fi exercitate;

d)Orice alte informații a căror furnizare este impusă prin dispoziție a ANSPDCP, ținând seama de specificul prelucrării.

IV. Toate informațiile privind starea pacientului, rezultatele investigațiilor, diagnosticul, tratamentul, datele personale sunt confidențiale chiar și după decesul acestuia.

V. În calitate de angajator, spitalul prelucrează date cu caracter personal ale candidaților și ale personalului angajat în vederea încheierii, desfășurării și/sau încetării raporturilor de muncă. Categoriile de date cu caracter personal prelucrate includ:

a)Date de identificare, contact, nume, prenume, cod numeric personal, data nașterii, telefon mobil

personal, adresa de e-mail, starea civilă, etc.;

b)Date privind experiența profesională: CV-uri, scrisoare de recomandare, adeverință vechime etc;

c)Date legate de studii, competențe: diplome, certificate de competență, certificate de specializare, polițe de asigurare pentru malpraxis, etc;

d)Date privind starea de sănătate: adeverința de la medicul de familie, certificat medical tip A5, etc;

e)Date despre infracțiuni sau condamnări definitive, acestea fiind solicitate doar cu respectarea prevederilor legale în vigoare.

f) Date financiare.

Prelucrarea datelor cu caracter personal în acest caz este realizată în vederea executării unui contract ce reglementează raportul de muncă (contractul individual de muncă, contractul de management, contract de administrare, contractul de voluntariat, etc.), și în vederea îndeplinirii obligațiilor legale ce îi revin instituției.

VI. Categoriile speciale de date - date despre starea de sănătate a persoanei vizate, necesare în scopuri legate de medicina preventivă sau a muncii, pentru evaluarea capacității de muncă a angajatului, diagnostic medical, sănătate sau asistență socială sunt prelucrate atunci când este necesar în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii Europene sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor (în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente).

VII. Prelucrările de date cu caracter personal se efectuează după informarea angajaților și a candidaților care se prezintă la concurs în vederea ocupării unui post vacant, de către serviciul RUNOS conform Notificării generale angajați privind prelucrarea datelor cu caracter personal – **Anexa 3**, și Notificarea generală candidați privind prelucrarea datelor cu caracter personal – **Anexa 4**.

Aceștia sunt informați în baza documentului de notificare generală privind prelucrarea datelor cu caracter personal, cu privire la:

a)Identitatea operatorului și a reprezentantului acestuia, dacă este cazul;

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM	
	Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	
	Ediția: 1	Revizia: 0
	Exemplar nr.1	

- b) Scopul în care se face prelucrarea datelor;
- c) Informații suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie și consecințele refuzului de a le furniza; existența drepturilor de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care pot fi exercitate;
- d) Orice alte informații a căror furnizare este impusă prin dispoziție a ANSPDCP ținând seama de specificul prelucrării.

VIII. Prin intermediul sistemelor de supraveghere video, spitalul prelucrează datele cu caracter personal, respectiv imaginea și alte informații ce permit identificarea persoanelor. Prelucrarea datelor cu caracter personal se face având ca temei legal îndeplinirea obligațiilor legale și realizarea intereselor legitime. Scopul prelucrării datelor personale constă în: monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor, prevenirea și/sau combaterea infracțiunilor.

IX. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se realizează numai de către persoane autorizate (numite prin decizia Managerului SPMS JEBEL). Personalul nominalizat respectă setările de confidențialitate și drepturile de acces. Accesul este strict limitat la angajații ce accesează, în spațiul unde se află, echipamentele de înregistrare și stocare ale sistemului de supraveghere video.

X. Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video este de maxim 30 de zile calendaristice, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate. La expirarea termenului înregistrările se distrug automat prin procesul de suprascriere.

Persoanele vizate, respectiv pacienții, angajații, vizitatorii și alte persoane care intră în incinta spitalului sunt informate în legătură cu prelucrarea datelor personale prin intermediul sistemelor de supraveghere video prin afișarea informărilor în cauză (**Anexa 5 – Infografic supraveghere video**), precum și a indicatoarele de marcare a existenței sistemului de supraveghere video, în locurile unde sunt amplasate camere de supraveghere video.

XI. Dacă prelucrarea datelor cu caracter personal depășește scopul acordării serviciului medical sau al protejării interesului vital al pacientului, este necesar consimțământul (De exemplu: pentru participarea în procesul de învățământ medical, pentru filmarea unei proceduri – una care nu este în scop medical, pentru marketing direct, pentru folosirea unui testimonial, pentru promovarea imaginii spitalului etc).

XII. Pentru obținerea consimțământului pacientului pentru prelucrarea datelor cu caracter personal se va folosi ” **Acord privind prelucrarea datelor cu caracter personal** ” – **Anexa 6.**

Consimțământul pentru prelucrarea datelor conform GDPR vizează strict prelucrarea datelor cu caracter personal, fiind separat de Consimțământul medical informat ce vizează relația medic-pacient și informațiile legate de actul medical și repercusiunile acestuia.

C. Înregistrarea datelor

I. Înregistrarea datelor cu caracter personal este realizată la nivelul spitalului astfel:

- a) La internare, operatorii (registratorul medical/ asistentul de serviciu/ asistentul șef) introduc datele de identificare ale pacienților în format electronic, în cadrul platformei informatice utilizată la nivelul spitalului;
- b) După completarea datelor cu caracter personal ale pacienților/apartenențelor în sistemul informatic, aceleași date sunt consemnate de către personalul medico-sanitar în cadrul documentelor fizice

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

(FSZ/FOCG, plan de îngrijire, etc), cu scopul menținerii evidenței la zi a evoluției stării de sănătate a pacientului.

- c) Prin înregistrarea în format electronic a datelor personale din FOCG, este colectat setul minim de date la nivel de pacient aferent spitalizării continue, format din datele clinice la nivel de pacient și setul minim de date la nivel de pacient, aferent spitalizării de zi, format din datele clinice la nivel de pacient care se colectează electronic din FSZ.
- d) Cu ocazia efectuării investigațiilor recomandate, rezultatele acestora sunt transmise atât în format fizic, cât și prin intermediul sistemului informatic. Aceste informații fac parte din setul de date cu caracter personal ce sunt păstrate în dosarul medical iar personalul cu drept de acces la acestea au obligația respectării confidențialității acestora, cu excepția situațiilor prevăzute în mod expres de legislația în vigoare.
 - II. Operatorii (asistenți de serviciu, asistenți șef, medici, registratori medicali) sunt împuterniciți pentru a prelucra aceste date ale pacienților, au user și parolă personalizate/personalizabile și au obligația de a nu le divulga.
 - III. Completarea bazei de date și actualizarea acesteia este necesară în vederea acumulării progresive și constante a datelor despre pacienți. Baza de date este securizată (parola de utilizare) și utilizată doar de către personalul abilitat în acest sens (Serviciul de Evaluare și Statistică Medicală din cadrul spitalului, medici curanți, asistenți medicali și registratori medicali din spital, psihologi, asistenți sociali etc.).
 - IV. Operatorii au obligativitatea privind confidențialitatea datelor medicale, a utilizării acestora numai în scopurile specificate și a informării pacienților privind prelucrarea statistică a datelor colectate în fișele de observație și în fișele de prezentare, obligații specificate și în cadrul fișelor de post.
 - V. Datele cu caracter personal ale angajaților sau ale potențialilor angajați sunt prelucrate de către angajații serviciului RUNOS, aceștia având obligația respectării confidențialității acestor date.

D. Accesarea dosarului personal medical

- I. În conformitate cu legislația specifică în vigoare, pacientul are acces la datele medicale personale, spitalul având obligația de a asigura pacienților accesul neîngrădit la aceste date. Condițiile eliberării duplicatelor (modalitate de solicitare, circuit documente, responsabili, timp de răspuns și modalitate de transmitere) documentelor menționate sunt consemnate în procedura specifică privind comunicarea internă și externă. Orice pacient sau fost pacient are acces la toată documentația medicală din serviciile unde a fost îngrijit, cu excepția cazurilor în care:
 - a) dezvăluirea unor asemenea documente medicale ar putea să fie în detrimentul sănătății sale fizice și mintale, acest fapt fiind stabilit de către medicul-șef sau de către medicul curant;
 - b) a fost efectuată o specificație scrisă asupra riscului acestui efect pe dosarul pacientului, aplicată numai persoanelor care sunt pacienți în prezent, nu și foștilor pacienți.
- II. Fiecare membru din echipa terapeutică este obligat să păstreze confidențialitatea informațiilor, cu excepția următoarelor situații:
 - a) există o dispoziție legală în acest sens;
 - b) sunt necesare pentru stabilirea vinovăției în cazul unei infracțiuni prevăzute de lege;
 - c) există acordul scris al persoanei în cauză;

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

- d) sunt necesare pentru exercitarea profesiei, cu condiția respectării anonimatului persoanei în cauză;
- e) este necesară transmiterea acestora între diferite unități sanitare, la cerere sau cu ocazia transferului, dacă pacientul acceptă transferul;
- f) când anumite informații referitoare la un tratament actual sau trecut privind un pacient sunt necesare unei instanțe de judecată sau Colegiului Medicilor din România, care judecă în legătură cu o cauză, medicul curant este autorizat să aducă dovezi de orice fel privind pacientul și comunicări ale informațiilor aflate sub semnul confidențialității.

III. SPMS JEBEL administrează în condiții de siguranță și numai pentru scopurile specificate, datele personale pe care le furnizează personalul angajat/contractual ori potențialii angajați, și pe cele ale pacienților despre ei înșiși, despre un membru al familiei sau altă persoană, .

IV. Atât pacienții cât și angajații beneficiază de dreptul de acces, de intervenție asupra datelor, dreptul de a nu fi supus unei decizii individuale și dreptul de a se adresa justiției.

i. Dacă pacientul constată faptul că unele din datele sale personale sunt incorecte, acesta informează spitalul prin completarea și transmiterea formularului “**Cerere persoană vizată**” – Anexa 7, pentru a remedia eroarea (în cazul în care pacientul este internat, acesta informează verbal personalul secției). În cazul în care pacientul/apartinătorul constată neconformități după externarea pacientului, acesta poate transmite formularul:

- a) prin email la adresa secretariat@spitaljebel.ro; personalul Compartimentului de Relații cu Publicul transmite cererea către secția unde pacientul a fost internat pentru operarea modificărilor, responsabil cu operarea modificărilor fiind registratorul de serviciu;
- b) prin poștă la adresa Jebel, Jud. Timiș, Cod postal 307235, România , urmând circuitul descris la litera a)

ii. Dacă personalul angajat/potențial angajat constată că unele din datele sale personale sunt incorecte, acesta informează spitalul fie direct prin comunicarea cu personalul RUNOS (în cazul personalului angajat), fie prin completarea și transmiterea formularului “**Cerere persoană vizată**” – Anexa 7, pentru a remedia eroarea. Formularul se poate transmite:

- a) prin email la adresa runos@spitaljebel.ro; personalul RUNOS având obligația verificării datelor și actualizarea acestora, după caz;
- b) prin poștă la adresa Jebel, Jud. Timiș, Cod postal 307235, România.

V. Orice persoană are dreptul de a se opune, pentru motive legitime, la prelucrarea datelor ce o privesc prin completarea formularului “**Cerere persoană vizată**” – Anexa 7 . Acest drept de opoziție poate fi exclus pentru anumite prelucrări prevăzute de lege (de ex.: prelucrări efectuate de serviciile financiare și fiscale, de poliție, justiție, securitate socială, cercetare științifică sau istorică). Prin urmare, această mențiune nu poate figura dacă prelucrarea are un caracter obligatoriu. Orice persoană are, de asemenea, dreptul de a se opune, în mod gratuit și fără nicio justificare, la prelucrarea datelor sale personale în scopuri de marketing direct prin retragerea consimțământului. În sensul retragerii consimțământului anterior exprimat privind prelucrarea datelor cu caracter personal pentru alte scopuri decât cele cuprinse în cadrul Anexei 2 la prezenta PS, persoana vizată completează Anexa 7 la prezenta, în conformitate cu solicitările dorite și transmite formularul către DPO-ul spitalului, pe adresa de email dpo@spitaljebel.ro.

VI. Informațiile cu caracter confidențial pot fi furnizate terților numai în cazul în care pacientul își exprimă consimțământul explicit, în conformitate cu prevederile procedurii documentate aplicabilă la nivelul spitalului privind acordul pacientului informat, sau în cazurile în care legea o cere în mod expres, fără a mai fi necesar acordul pacientului. În situațiile în care informațiile sunt necesare altor

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

furnizori de servicii medicale acreditați, implicați în tratamentul pacientului, acordarea consimțământului nu mai este obligatorie.

- VII.** Datele cu caracter personal prelucrate de către spital sunt destinate utilizării de către acesta, însă parte din activitățile acestuia presupune transmiterea acestor date către alte instituții și/sau autorități publice cum sunt: Casa Națională de Asigurări de Sănătate - C.N.A.S., Direcția de Sănătate Publică - D.S.P., Dosarul Electronic de Sănătate - D.E.S., Autoritatea Națională de Management al Calității în Sănătate - A.N.M.C.S., Inspectoratul Teritorial de Muncă - I.T.M., Agenția Națională de Administrare Fiscală - A.N.A.F., Instituția Poliției, Parchet, Tribunal, Judecătoria, etc.
- VIII.** SPMS JEBEL nu transferă datele cu caracter personal ale persoanelor vizate în afara Spațiului Economic European, cu excepția cazului în care se asigură un nivel adecvat de protecție. Protecția conferită de Regulamentul general privind protecția datelor însoțește datele în călătoria lor, ceea ce înseamnă că normele care protejează datele continuă să se aplice indiferent unde ajung aceste date. Acest lucru este valabil și când datele se transferă într-o țară care nu este membră a Uniunii Europene (țară terță).
- IX.** Datele cu caracter personal sunt destinate utilizării de către spital, dar în anumite situații este posibilă divulgarea acestora, astfel:
- Către alți **furnizori de servicii**, cum sunt medicii colaboratori și alți furnizori de servicii medicale, în scopul îmbunătățirii calității serviciilor oferite de către spital și în interesul strict al sănătății pacientului.
 - În cazul unor **situații de urgență** sau cazuri de **forță majoră**, conform prevederilor legale.
- X.** Transferurile de date cu caracter personal într-o țară care nu este membră a Uniunii Europene se pot realiza în condițiile în care țara respectivă este declarată, printr-o decizie a Comisiei Europene, ca oferind un nivel de protecție adecvat; în absența unei decizii privind caracterul adecvat al nivelului de protecție, transferul se poate face prin asigurarea unor garanții adecvate și cu condiția ca persoanele fizice să beneficieze de drepturi opozabile și de căi de atac eficace. Printre asemenea garanții adecvate se numără, de exemplu, clauzele contractuale standard.
- XI.** În cazul în care se realizează transferuri de date cu caracter personal către o țară terță, persoanele vizate sunt informate de către spital. De asemenea sunt informate și despre existența sau absența unei decizii a Comisiei Europene privind caracterul adecvat sau o trimitere la garanțiile adecvate.
- XII.** Pentru exercitarea drepturilor prevăzute de legislația specifică și de prezenta procedură, persoanele vizate se pot adresa Responsabilului cu protecția datelor din cadrul SPMS JEBEL, prin completarea formularului "Cerere persoană vizată" – Anexa 7, la adresa de e-mail: dpo@spitaljebel.ro sau la următoarea adresă de corespondență: Jebel, Jud. Timiș, Cod postal 307235, România
- Responsabilul cu protecția datelor din cadrul SPMS JEBEL, înregistrează formularele "Cerere persoană vizată" transmise de către persoanele vizate în "**Registrul privind cererile persoanelor vizate**" – **Anexa 8**. Răspunsurile cererilor persoanelor vizate sunt întocmite în colaborare cu personalul spitalului și vor fi întotdeauna vizate de către Managerul spitalului.
- XIII.** SPMS JEBEL, în calitate de operator de date cu caracter personal, are obligativitatea de a identifica persoana fizică care înaintează cererea prin intermediul căreia își exercită drepturile de care beneficiază, prin solicitarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate (ex: copie carnet asigurat, copie carte de identitate, pașaport etc).

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

XIV. SPMS JEBEL furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri prin care își exercită drepturile de care beneficiază în baza legii, fără întârzieri nejustificate și în orice caz în cel mult o lună calendaristică de la data primirii cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor.

XV. În cazul în care conducerea SPMS JEBEL consideră oportună prelungirea perioadei pentru formularea unui răspuns, SPMS JEBEL informează persoana vizată cu privire la aceasta, în termen de maximum o lună de la data primirii cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format. Dacă SPMS JEBEL nu poate dispune măsuri cu privire la obiectul cererii persoanei vizate, acesta informează persoana vizată, fără întârziere și în termen de cel mult o lună calendaristică de la data primirii cererii, cu privire la motivele inacțiunii și prezintă posibilitatea de a depune o plângere în fața ANSPDCP.

XVI. Informațiile furnizate în temeiul legislației specifice și orice comunicare/măsuri adoptate în baza exercitării drepturilor de care beneficiază persoana vizată, în condițiile legii, sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, spitalul poate să refuze să dea curs cererii. În aceste cazuri, spitalului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

E. Accesul la datele cu caracter personal ale angajaților

I. Documentele ce conțin date cu caracter personal ale angajaților sunt înregistrate în general de către personalul serviciului RUNOS, iar în particular de către șefii/coordonatorii compartimentelor din spital. Documentele cu caracter personal sunt păstrate în locații fizice sigure și corespunzătoare. Documentele, terminalele de acces/echipamentele care conțin date cu caracter personal sunt ținute/păstrate în fișete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare și/sau în încăperi/spații care se pot încuia.

Doar persoanele autorizate au acces la documente și doar în scopul realizării responsabilităților structurii în care își desfășoară activitatea.

II. Accesarea datelor cu caracter personal stocate în aplicațiile interne se realizează doar pe baza unui user și a unei parole atribuite fiecărui angajat autorizat în acest sens.

III. Personalul angajat în cadrul spitalului are dreptul de acces la propriile date cu caracter personal pe care spitalul le prelucrează. Pentru a solicita aceste date (sub formă de adeverință, extras din revisal etc.), personalul angajat formulează o cerere și o transmite serviciului RUNOS, în conformitate cu procedura privind comunicarea internă și externă.

F. Măsuri tehnice de asigurare a securității prelucrării datelor cu caracter personal

Accesul atât la terminalele PC, cât și la documentele fizice care conțin date cu caracter personal este permis doar personalului autorizat (medici, asistenți medicali, registratori medicali, statisticieni, etc) și doar pentru exercitarea atribuțiilor de serviciu.

Utilizarea datelor cu caracter personal de către spital este în conformitate cu reglementările legale în vigoare și ține cont de protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date și cuprinde următoarele etape:

I. Identificarea și autentificarea utilizatorului sistemului informatic.

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

1. Prin utilizator se înțelege orice persoană care acționează sub autoritatea spitalului sau a persoanei împuternicite, cu drept recunoscut de acces la bazele de date cu caracter personal.
 2. Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, este necesar să se identifice. În cadrul spitalului identificarea se face cu ajutorul unui user și a unei parole, folosite pentru autentificarea user-ului respectiv; fiecare utilizator având propriul user și parolă. Niciodată nu este alocat același user mai multor utilizatori.
 3. Orice utilizator care primește un cod de identificare și un mijloc de autentificare este obligat să păstreze confidențialitatea acestora și să răspundă în fața operatorului.
 4. Codurile de identificare sau conturile de utilizator (user și parole) nefolosite o perioadă mai îndelungată sunt dezactivate și distruse după un control intern prealabil efectuat de specialiștii din cadrul compartimentului IT al spitalului.
 5. Parolele sunt schimbate periodic în funcție de politicile de securitate stabilite de departamentul IT. Schimbarea periodică a parolelor se face numai de către utilizatorii autorizați de operator, cu o notificare ulterioară a departamentului IT, responsabil cu securitatea sistemului informatic. Departamentul IT realizează o evidență a conturilor de utilizatori din cadrul spitalului.
- II. Obligațiile specifice ale utilizatorilor sistemului informatic. Utilizatorii bazelor de date cu caracter personal au următoarele obligații:**
1. Să cunoască și să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum și cele ale procedurilor interne în vigoare;
 2. Să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condițiile legii, cu privire la: identificarea operatorului (spitalului), scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute și consecințele refuzului de a le pune la dispoziție, drepturile prevăzute de lege, în special drepturile de acces, de intervenție asupra datelor și de opoziție, condițiile în care pot fi exercitate aceste drepturi;
 3. Să prelucreze numai date cu caracter personal necesare îndeplinirii atribuțiilor de serviciu;
 4. Să păstreze confidențialitatea datelor prelucrate, a contului de utilizator și a parolei/codului de acces la sistemele informatice/ baza de date prin care sunt gestionate datele cu caracter personal;
 5. Să respecte măsurile de securitate precum și celelalte reguli stabilite de către conducerea spitalului;
 6. Să informeze cu prioritate, în scris, responsabilul cu protecția datelor și conducerea spitalului în cazul în care sesizează circumstanțe de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre posibile situații de încălcare a normelor legale situații privind accesul/prelucrarea de date cu caracter personal.
- III. Tipul de acces**
1. Utilizatorii pot accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu și sunt obligați să păstreze confidențialitatea acestora. Pentru aceasta sunt stabilite tipurile de acces după funcționalitate (administrare, introducere, prelucrare, salvare, etc.) și după acțiuni aplicate asupra datelor cu caracter personal (scriere, citire, ștergere).

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

2. În situația unor cazuri excepționale constând în intervenția compartimentului sau persoanei cu atribuții pentru asigurarea suportului tehnic și IT, intervenții ce presupun accesul la date cu caracter personal, acestea se realizează cu respectarea confidențialității datelor.
3. Alte măsuri specifice implementate de control al accesului sunt:
 - a) în cadrul instituției sunt instalate sisteme de supraveghere video;
 - b) Monitorizarea accesului persoanelor și autovehiculelor în cadrul spitalului se face de către agenții firmei de pază (serviciu externalizat).

IV. Executarea copiilor de siguranță

Pentru bazele de date cu caracter personal precum și pentru programele folosite pentru prelucrările automatizate se generează zilnic, în mod automat de către sistemul informatic, copii de siguranță (back-up) pentru o eventuala recuperare a datelor în cazul distrugerii sau disfuncționalității sistemelor informatice.

V. Computerele și terminalele de acces

1. Computerele și terminalele de acces sunt protejate cu parolă.
2. Computerele și alte terminale de acces sunt instalate în încăperi cu acces restricționat. Orice sesiune de lucru asupra căreia nu se acționează o perioadă de 30 de secunde intră automat în modulul stand-by, iar conturile de utilizator vor fi protejate de parole personalizate, cunoscute doar de către aceștia.
3. Terminalele de acces folosite în relația cu publicul pe care apar date cu caracter personal vor fi poziționate astfel încât să nu poată fi văzute de public.
4. Serverele care găzduiesc bazele de date pot fi accesate doar în mod controlat și doar de către specialiștii din cadrul departamentului IT al spitalului (ori de către personalul autorizat al firmei contractoare) și nu pot fi accesate din afara rețelei spitalului.
5. Nu este permisă utilizarea mediilor de stocare personale.
6. Nu este permisă scoaterea din instituție a mediilor de stocare mobile (CD/DVD, USB, STICK, Portable HDD, etc), decât cu aprobarea scrisă, prealabilă, din partea conducerii spitalului.
7. Angajaților le este interzisă utilizarea aplicațiilor bazate pe cloud sau copii de rezervă care să permită transferul datelor legate de instituție către terți. Angajații nu folosesc pe dispozitivele electronice personale mobile servicii de mesagerie online (exemplu: WhatsApp, Facebook Messenger, Telegram, ș.a.m.d.) în desfășurarea activității profesionale.

VI. Fișierele de acces

1. La nivelul spitalului accesul la bazele electronice de date cu caracter personal sunt înregistrate într- un fișier de acces (numit log la prelucrările automate), iar pentru prelucrările manuale de date cu caracter personal acestora sunt consemnate în registru.
2. Informațiile înregistrate în fișierul de acces sau în registru sunt:
 - i. Codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manual);
 - ii. Numele fișierului accesat (fișei);
 - iii. Numărul înregistrărilor efectuate;
 - iv. Tipul de acces;

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

- v. Codul operației executate sau programul folosit;
- vi. Data accesului (an, luna, zi);
- vii. Timpul (ora, minutul, secunda)

3. Pentru prelucrările automate aceste informații sunt stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator. De asemenea, orice încercare de acces este înregistrată. Fișierele de acces fac posibilă identificarea de către spital, sau de către persoana împuternicită de către acesta, a persoanelor care au accesat neautorizat date cu caracter personal, în vederea aplicării unor sancțiuni sau a sesizării organelor competente, după caz.

G. Instruirea personalului

1. În cadrul spitalului personalul angajat este informat de către DPO, prin sesiuni de instruire periodice semestriale, cu privire la prevederile Regulamentului General (UE) nr.679/2016 pentru protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității desfășurate la nivelul fiecărei secții/compartiment/birou/serviciu, conform calendarului anual de instruire specific activității.
2. Anual, nu mai tarziu de sfârșitul luni decembrie a fiecărui an, DPO-ul întocmește calendarul de instruire privind aspectele menționate la punctul 1., având în vedere toate structurile din spital.
3. Instruirile personalului au în vedere atât regulamentul mai sus menționat, cât și prevederile prezentei PS.
4. Evaluând tipurile de riscuri, personalului i se aduc în vedere și tipul surselor ce pot genera aceste riscuri, și anume:
 - a) Sursa umană din interior: angajați, operatori interni, etc.
 - b) Sursa umană din exterior: destinatari ai datelor cu caracter personal, terțe părți autorizate, furnizorii de servicii, hackeri, vizitatori, ex-angajați, etc.
 - c) Surse ne-umane: malware (virusi), apa (conduce, inundații, infiltrații), substanțe inflamabile, corozive sau explozive, dezastre naturale, etc.
5. Utilizatorii care au acces la date cu caracter personal sunt informați, de către serviciul RUNOS prin **Informarea asupra obligațiilor angajaților în desfășurarea activităților de prelucrare a datelor cu caracter personal Anexa – 9**, asupra confidențialității acestora și sunt avertizați asupra obligativității respectării prevederilor Regulamentului General (UE) 2016/679.
6. Angajaților, studenților în practică, rezidenților, voluntarilor spitalului, li se interzice să utilizeze date cu caracter personal în scopuri personale sau comerciale, să le dezvăluie unor persoane neautorizate sau să le pună la dispoziție în orice alt mod. Aceștia semnează la angajare un **Acord de confidențialitate Anexa -10**, ce se păstrează la dosarul de personal al angajatului.

H. Vulnerabilități privind securitatea prelucrării datelor cu caracter personal.

1. În ceea ce privește prelucrarea și protecția datelor cu caracter personal la nivelul sistemului informatic au fost identificate următoarele vulnerabilități și sunt prevăzute următoarele măsuri pentru limitarea acestora:

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

1. *Utilizarea programelor software care provin din surse externe sau dubioase - este interzisă folosirea de către utilizatori a acestor tipuri de programe;*
2. *Accesul, listarea și transmiterea documentelor care conțin date cu caracter personal de către persoanele neautorizate în acest sens - prelucrarea datelor cu caracter personal se realizează numai de către utilizatori autorizați de către spital pentru execuția acestor operațiuni.*
3. *Infectarea terminalelor de acces cu viruși informatici – în cadrul sesiunilor de instructaj, DPO Informează utilizatorilor în privința pericolului privind virușii informatici;*
4. *Utilizarea terminalelor de acces de la nivelul spitalului care nu folosesc sistem de operare cu licență (Windows Defender) - Implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;*
5. *Prelucrarea, păstrarea, arhivarea și/sau distrugerea documentelor fără a fi supuse circuitului stabilit în spital - toate documentele (care conțin date cu caracter personal) sunt înregistrate și urmează regulile de păstrare, procesare, multiplicare, transport, transmitere, arhivare și distrugere stabilite prin Legea Arhivelor Naționale și prin procedurile interne privind arhivarea documentelor; Arhivarea electronică se realizează pe serverul spitalului.*
6. *Accesul persoanelor neautorizate în încăperile în care se afla documente ce conțin date cu caracter personal și/sau echipamente care prelucrează date cu caracter personal – accesul în astfel de încăperi este strict limitat la utilizatorii autorizați de către conducerea spitalului și numai pentru îndeplinirea atribuțiilor de serviciu, în acest sens încăperile dispun de sisteme de securizare a căilor de acces.*
7. *Accesul persoanelor neautorizate la aplicațiile informatice care gestionează date cu caracter personal - aplicațiile informatice care gestionează date cu caracter personal sunt prevăzute cu facilitatea închiderii automate a sesiunii de lucru dacă utilizatorul nu acționează asupra datelor afișate pe ecran o perioadă de timp de până la 40 minute, stabilită în funcție de operațiile care trebuie executate pentru fiecare tip de prelucrare în parte;*
8. *Transmiterea datelor cu caracter personal către terți fără a se respecta cerințele minime de securitate – datele se criptează înainte de transmitere (acolo unde este cazul) și se transmit prin poștă, prin intermediul adreselor de email instituționale către adresele comunicate în cadrul solicitărilor, predare personală, după caz.*

II. În ceea ce privește prelucrarea și protecția datelor cu caracter personal ce privesc documentele în format fizic au fost identificate următoarele vulnerabilități și sunt prevăzute măsuri pentru limitarea acestora:

1. *Imprimarea de către personal neautorizat a documentelor ce conțin date cu caracter personal – aceasta operațiune se realizează doar de către acei utilizatori autorizați în acest sens. De asemenea, documentele care sunt recepționate sau se transmit pe fax din secretariatul instituției se operează cu respectarea confidențialității datelor, în sensul că acestea nu se lasă la îndemâna persoanelor neautorizate (public sau alți angajați).*
2. *Distrugerea improprie/parțială a documentelor care conțin date cu caracter personal (nu se referă la casarea documentelor) – în sensul diminuării riscului de reconstituire a documentelor, această operațiune se realizează doar cu ajutorul distrugătorului de hârtie.*
3. *Depozitarea improprie a documentelor cu caracter personal arhivate – documentele arhivate sunt depozitate doar în spații special amenajate la care accesul este restricționat, iar îndosărierea și inventarierea arhivei se face conform legii.*
4. *Documentele ce conțin date cu caracter personal care nu au fost îndosariate, inventariate și/sau depozitate corespunzător în arhiva temporară sunt ținute în spații la care pacienții sau oricare*

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM	
	Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	
	Ediția: 1	Revizia: 0
	Exemplar nr.1	

alte persoane neautorizate ar putea avea acces – depozitarea temporară/definitivă a documentelor este reglementată prin proceduri specifice implementate la nivelul spitalului (dulapuri încuiate, încăperi cu acces limitat etc).

5. *Menționarea datelor cu caracter personal pe bibliorafturi/dosare/mape la care pacienții/persoane neautorizate ar putea avea acces – pe acele bibliorafturi/dosare/mape care circulă în mod frecvent la nivelul spitalului și la care ar putea avea acces persoane neautorizate nu se consemnează date cu caracter personal.*
6. *Accesul personalului neautorizat în spațiul destinat depozitării documentelor arhivate; consultarea documentelor ce conțin date cu caracter personal și realizarea duplicatelor fără acordul managementului spitalului – în incinta Arhivei spitalului are acces doar personalul autorizat. Persoanele care doresc acces la documentele arhivate pot obține permisiunea managementului spitalului în condițiile precizate în procedura specifică implementată la nivelul unității și doar în scopurile menționate în aceasta.*
7. *Libera circulație a documentelor – la nivelul spitalului este interzisă, prin proceduri documentate specifice, transmiterea/părăsirea spitalului a documentelor fără avizul managementului în acest sens.*
8. *Consultarea arhivei fără respectarea normelor privind buna gestionare a documentelor – la nivelul spitalului este reglementată interdicția de a descompleta documentele arhivate ori de a distruge parte sau tot din acestea, cu excepția casării în condițiile legii.*

1. Responsabilul cu protecția datelor cu caracter personal (DPO)

1. Responsabilul cu protecția datelor monitorizează respectarea Regulamentului General privind protecția Datelor. DPO-ul efectuează audituri aferente operațiunilor de prelucrare și familiarizează angajații spitalului cu conținutul procedurii privind protecția datelor cu caracter personal prin sesiuni de instruire.
2. Pentru planurile de prelucrare a datelor care pot prezenta riscuri speciale pentru drepturile individuale ale persoanelor vizate, DPO-ul este informat anterior de către spital înainte de începerea prelucrării, prin intermediul adresei de email prezentată mai jos ori telefonic. Acest aspect se aplică în mod obligatoriu prelucrării datelor cu caracter personal sensibile.
3. Responsabilul cu protecția datelor (DPO) fiind independent din punct de vedere al ordinilor profesionale, își desfășoară activitatea pentru respectarea legislației în vigoare privind protecția datelor cu caracter personal. El este responsabil pentru întocmirea, evaluarea, revizuirea (după caz) și supravegherea respectării procedurii privind prelucrarea și protecția a datelor cu caracter personal.
4. Responsabilul cu protecția datelor are linie de raportare directă către managerul organizației.
5. Orice persoană vizată poate aborda DPO-ul, în orice moment, să ridice preocupări, să adreseze întrebări, să solicite informații sau să depună plângeri legate de protecția datelor sau de problemele de securitate a datelor. Dacă se solicită, preocupările și plângerile vor fi tratate în mod confidențial.
6. Deciziile luate de Responsabilul cu protecția datelor (DPO) pentru remedierea încălcărilor privind protecția datelor trebuie să fie susținute de conducerea spitalului.
7. Anchetele autorităților de supraveghere sunt întotdeauna raportate DPO-ului.
8. Toți angajații SPMS JEBEL sunt informați cu privire la rolul și poziția DPO-ului din cadrul instituției, de către conducătorii structurilor prin diseminarea în cadrul instituției a **Anexei 11 - Descrierea postului de responsabil cu protecția datelor cu caracter personal.**

Datele de contact ale DPO-ului sunt următoarele:

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

DPO Extern : SC DAF Consulting & Management SRL email : dpo@dafcons.ro

telefon : 0724.617.735

Persoana de contact : Responsabil cu protecția datelor – Dl. Dragoș TECIOIU email : dragos.tecioiu@dafcons.ro

telefon: 0723.141.821

J. Relația cu ANSPDCP

Persoanele vizate, din orice categorie ar face ele parte, pot sesiza sau face reclamații referitoare la situații de încălcare a prevederilor Regulamentului nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), adresate Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal care are sediul în București, str. General Gheorghe Magheru nr. 28-30, sector 1 și poate fi contactată la telefon 0318059211 sau adresa de mail anspdcpl@dataprotection.ro.

K. Notificarea încălcării securității datelor cu caracter personal

Regulamentul general privind protecția datelor introduce cerința ca o încălcare a securității datelor cu caracter personal (denumită în continuare „încălcare”) să fie notificată Autorității Naționale de Supraveghere competente și, în anumite cazuri, ca persoanele ale căror date cu caracter personal au fost afectate de încălcare să fie informate cu privire la aceasta. O încălcare a securității poate duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea în cadrul SPMS JEBEL.

Prin prezenta procedură se stabilește scopul îndrumării în eventualitatea producerii unei încălcări a securității datelor cu caracter personal și planul de răspuns la încălcări, precum și a atribuțiilor persoanelor implicate în procesul de notificare a Autorității de supraveghere și de informare a persoanelor vizate afectate.

1. Clasificarea încălcărilor de securitate

Încălcările pot fi clasificate în funcție de următoarele trei principii privind securitatea informațiilor:

- „Încălcarea confidențialității” – în cazul în care are loc o divulgare neautorizată sau accidentală sau un acces neautorizat sau accidental la datele cu caracter personal;
- „Încălcarea integrității” – în cazul în care are loc o modificare neautorizată sau accidentală a datelor cu caracter personal;
- „Încălcarea disponibilității” – în cazul în care are loc o pierdere accidentală sau neautorizată a accesului sau distrugerea datelor cu caracter personal.

De asemenea, în funcție de circumstanțe, o încălcare se poate referi în același timp la confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal, precum și la orice combinație a acestor elemente.

2. Detectarea încălcărilor securității datelor cu caracter personal și analiza acestora

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

În cazul încălcărilor de securitate detectate atât în mod automat cu ajutorul unor programe software ale SPMS JEBEL , cât și de către angajați, acestea se notifică către conducerea SPMS JEBEL și către Responsabilul cu protecția datelor. Un obiectiv important în ceea ce privește securitatea datelor cu caracter personal este reducerea intervalului de timp dintre producerea încălcării și momentul detectării acesteia.

Odată ce încălcarea a fost detectată, este necesară efectuarea unei analize inițiale de impact și o evaluare a riscurilor, pentru a decide care este răspunsul adecvat. În acest scop se va numi o echipă de răspuns la încălcări.

Analiza de impact trebuie să estimeze:

- impactul asupra infrastructurii IT, incluzând calculatoare, rețele și echipamente;
- datele cu caracter personal care ar putea fi supuse unui risc sau care ar putea fi compromise;
- durata probabilă a încălcării, de la producere până la detectare;
- compartimentele afectate și impactul asupra acestora;
- gradul de risc asupra drepturilor și libertăților persoanelor vizate în cazul încălcărilor ce privesc datele cu caracter personal;
- indicarea cauzei probabile a încălcării.

Este necesară o analiză temeinică pentru a se stabili cât mai clar momentul producerii și durata încălcării. De asemenea, se impune revizuirea analizei pe măsură ce apar noi informații în acest sens.

Metoda de evaluare a riscurilor

Deși RGPD introduce obligația de notificare a unei încălcări, nu este o cerință ca notificarea să fie efectuată în toate cazurile:

- notificarea autorității de supraveghere competente este obligatorie, cu excepția cazului în care este puțin probabil ca o încălcare să genereze un risc pentru drepturile și libertățile persoanelor;
- Informarea unei persoane cu privire la o încălcare este declanșată numai atunci când este posibil ca încălcarea să genereze un risc ridicat pentru drepturile și libertățile acesteia.

Aceasta înseamnă că, imediat după ce operatorul a luat cunoștință de o încălcare, este extrem de important ca acesta ar trebui nu numai să urmărească limitarea incidentului, ci și să evalueze riscul care ar putea decurge din acesta. Există două motive importante pentru aceasta: în primul rând, cunoașterea probabilității și a gravității potențiale a impactului asupra persoanei va sprijini operatorul să ia măsuri eficiente pentru a limita și a remedia încălcarea; în al doilea rând, aceasta îl va ajuta să stabilească dacă este necesară notificarea autorității de supraveghere și, dacă este necesar, a persoanelor în cauză.

Astfel cum s-a explicat mai sus, este necesară notificarea unei încălcări, cu excepția cazului în care este puțin probabil ca aceasta să genereze un risc pentru drepturile și libertățile persoanelor, iar elementul principal de declanșare care impune informarea persoanelor vizate cu privire la o încălcare este posibilitatea ca aceasta să genereze un *risc ridicat* la adresa drepturilor și libertăților persoanelor. Acest risc există atunci când încălcarea poate conduce la prejudicii de natură fizică, materială sau morală pentru persoanele ale căror date au fost afectate. Exemple de astfel de prejudicii includ discriminarea, furtul sau fraudă de identitate, pierderea financiară și compromiterea reputației. Atunci când încălcarea implică date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice sau apartenența la sindicate sau includ date genetice, date privind sănătatea sau date privind viața sexuală sau condamnări penale și infracțiuni sau măsuri de securitate conexe, ar trebui să se considere că este posibil să se producă prejudicii.

Factori de luat în considerare la evaluarea riscului

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	Ediția: 1	
	Revizia: 0	
	Exemplar nr.1	

RGPD sugerează că, în general, la evaluarea riscului ar trebui luată în considerare atât probabilitatea, cât și gravitatea riscului pentru drepturile și libertățile persoanelor vizate. Evaluarea ar trebui să țină seama de următoarele criterii:

- *Tipul încălcării*
- *Natura, sensibilitatea și volumul datelor cu caracter personal*
- *Ușurința identificării persoanelor*
- *Gravitatea consecințelor pentru persoane*
- *Caracteristici speciale ale persoanei*
- *Caracteristici speciale ale operatorului de date*
- *Numărul persoanelor afectate*
 - *Dacă datele personale au fost criptate și nivelul acesteia*

Rezultatul evaluării riscurilor ar trebui să includă una dintre următoarele concluzii:

- *Încălcarea datelor cu caracter personal nu necesită notificare;*
- *Încălcarea datelor cu caracter personal solicită doar notificarea autorității de supraveghere;*
- *Încălcarea datelor cu caracter personal necesită notificarea atât a autorității de supraveghere, cât și a persoanelor vizate afectate.*

3. Activarea planului de răspuns la încălcarea securității

Odată informat în legătură cu producerea unei încălcări, Responsabilul cu Protecția Datelor trebuie să decidă dacă gravitatea, mărimea, impactul actual sau potențial al acestuia justifică activarea planului de răspuns în cazul unei încălcări a securității și să convoace echipa de răspuns.

În acest sens, trebuie să aibă în vedere următoarele aspecte:

- există o pierdere semnificativă de informații (inclusiv date cu caracter personal), actuală sau potențială;
- există un risc semnificativ, actual sau potențial de perturbare a bunei funcționări a instituției;
- există un risc semnificativ de afectare a imaginii instituției;
- orice altă situație care ar putea avea un impact semnificativ asupra instituției.

4. Echipa de răspuns

În urma activării procedurii de răspuns, Responsabilul cu Protecția Datelor va convoca toți membrii și le va aduce la cunoștință încălcarea securității. Echipa de Răspuns poate începe să adune informații pentru analiza încălcării de îndată ce s-a constatat producerea sa, pentru ca o soluție adecvată să fie identificată în cel mai scurt timp posibil.

5. Numirea membrilor echipei de răspuns

Echipa de Răspuns trebuie să fie multidisciplinară, alcătuită din angajați care ocupă posturi ce necesită specializare juridică, economică, administrativă etc.

Exemplu structură Echipa de Răspuns:

Rol/Aria de Activitate	Rolul principal deținut
Responsabilul cu Protecția Datelor	Coordonator

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

Serviciul Economic	Director financiar contabil
Compartimentul Resurse umane	Șef serviciu RUNOS
Biroul Administrativ și Secretariat	Sef seerviciu ADMINISTRATIV
Sectii medicale	Director medical

Conducerea SPMS JEBEL numește Membrii Echipei de Răspuns prin decizie.

Responsabilul cu Protecția Datelor poate desemna personal suplimentar, cu acordul conducerii, în scopul soluționării unei încălcări a datelor cu caracter personal.

Nu este obligatoriu ca Echipa de Răspuns să implementeze soluționarea încălcărilor de securitate a informațiilor cu participarea tuturor membrilor. Se impune însă ca membrii să fie implicați, dacă incidentul produs are legătură directă cu domeniul lor de activitate.

De asemenea, Echipa de Răspuns va ține un jurnal al înregistrărilor privind acțiunile întreprinse. Este necesară completarea unui **Registru de măsuri cu toate informațiile relevante - Anexa nr. 12**. Trebuie păstrate și copii ale oricărei corespondențe referitoare la încălcare.

6. Notificarea ANSPDCP

În cazul în care apare o încălcare a securității datelor cu caracter personal care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, SPMS JEBEL va notifica acest lucru Autorității de Supraveghere (ANSPDCP), în termen de maxim 72 de ore de la momentul identificării.

Notificarea încălcării securității către Autoritatea de Supraveghere se va face prin intermediul formularelor online disponibile de pe site-ul web al acesteia www.dataprotection.ro/formulare/formularbresagdpr.

Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

O confirmare scrisă trebuie obținută de la Autoritatea de Supraveghere (ANSPDCP) privind notificarea trimisă, inclusiv data și ora la care aceasta a fost primită.

Notificarea ANSPDCP nu se impune în situația în care în urma evaluării impactului generat de incidentul de securitate asupra persoanelor vizate se constată că nu există niciun risc pentru drepturile și libertățile acestora.

Orice încălcare a securității (indiferent de riscul generat asupra persoanelor vizate) trebuie înregistrat în documentul **Registru incidente de securitate - Anexa 13**, care se păstrează de către Responsabilul cu protecția datelor (DPO) și de către Operator. Documentul **Recomandări întocmire incidente de securitate - Anexa 14**, propune structura registrului de mai sus și cuprinde o listă de exemple non-exhaustive cu scopul de a ajuta Operatorul în luarea deciziei dacă este necesară notificarea încălcărilor securității în diferite situații. Pentru a stabili și identifica mai ușor pași privind notificare încălcărilor de securitate a datelor cu caracter personal **Anexa 15 propune o Diagramă a cerințelor de notificare**.

Datele de contact ale ANSPDCP:

Adresa: B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, cod poștal 010336, București

Telefon: +40.318.059.211 +40.318.059.212

Fax: +40.318.059.220

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

E-mail: anspdcp@dataprotection.ro

Web: www.dataprotection.ro

7. Informarea persoanelor vizate cu privire la încălcările de securitate

În cazul în care încălcarea securității asupra datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, SPMS JEBEL va informa persoanele vizate în cel mai scurt timp, fără alte întârzieri, prin documentul **Formular de notificare a încălcării securității datelor către persoanele vizate – Anexa 16**.

Evaluarea riscurilor efectuată anterior în această procedură va determina dacă riscul pentru drepturile și libertățile persoanelor vizate afectate este considerat suficient de ridicat pentru a justifica notificarea acestora.

Informarea transmisă persoanelor vizate afectate va cuprinde următoarele informații:

- descrierea încălcării securității care afectează persoana vizată utilizând-se un limbaj clar și simplu, pe înțelesul persoanelor vizate afectate;
- numele și datele de contact ale DPO-ului - Responsabilul cu protecția datelor;
- descrierea succintă a eventualelor consecințe pentru persoanele vizate în urma încălcării securității;
- descrierea măsurilor deja implementate sau planificate pentru remedierea încălcării securității și, dacă este cazul, măsurile luate pentru atenuarea efectelor negative asupra persoanelor vizate.

Informarea persoanelor vizate nu este necesară dacă este îndeplinită oricare dintre următoarele condiții:

- au fost implementate măsuri tehnice și organizatorice adecvate în cazul datelor cu caracter personal afectate de încălcarea securității, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea sau pseudonimizarea;
- după identificarea încălcării securității au fost luate măsuri prin care se asigura că riscul ridicat pentru drepturile și libertățile persoanelor vizate afectate nu mai este susceptibil să se materializeze;
- efortul implicat este disproporționat cu scopul, în acest caz, se apelează la o informare publică sau se adoptă o măsură similară pentru informarea persoanelor vizate într-un mod la fel de eficace.

În majoritatea cazurilor, este oportun să se notifice persoanele vizate afectate prin scrisoare, e-mail sau ambele, pentru a se asigura că mesajul a fost primit și că aceștia au posibilitatea de a lua orice acțiune necesară.

8. Finalitatea planului de răspuns

Echipa de Răspuns va întocmi un raport final și va documenta activitățile, măsurile, persoanele implicate și datele cu caracter personal implicate aparținând persoanelor vizate, raport pe care-l va înainta conducerii SPMS JEBEL.

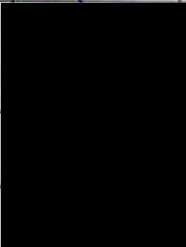
8. Responsabilități în derularea activității procedurale

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL		Ediția: 1
			Revizia: 0
			Exemplar nr.1

9. Formular de evidență a modificărilor procedurii

Nr. crt.	Numărul și data ediției	Numărul și data reviziei	Numărul paginii unde s-a efectuat modificarea	Descrierea modificării	Avizul conducătorului compartimentului în cadrul căruia s-a elaborat procedura
	1	2	3	4	5
1.	Ediția I 25.02.2026				
2.		Revizia 1/.....	Pag.	Modificarea, completarea	
3.		Revizia 2/.....	Pag.	Modificarea, completarea	
4.		Revizia n./.....	Pag.		
5.	Ediția II				
6.		Revizia 1/.....	Pag.		
7.		Revizia 2/.....	Pag.		
8.		Revizia n./.....	Pag.		

10. Formular de analiză a procedurii

Nr.Crt.	Compartiment	Nume si prenume conducător compartiment	Aviz favorabil		Aviz nefavorabil		
			Semnatura	Data	Observații	Semnatura	Data
1	Director financiar contabil	Albeanu Gelu		25.02.2026			
2	Director medical	Tanase Elena		25.02.2026			

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

11. Formular de difuzare a procedurii

Nr. EX.	Compartiment	Nume si prenume	Data primirii	Semnatura	Data retragerii procedurii inlocuite	Semnatura	Data intrarii in vigoare
1	Exemplarul nr. 1 (originalul) se păstrează la Comisia de Monitorizare, în cazul procedurilor de sistem și la compartimentul inițiator, în cazul procedurilor operaționale						
2	BIROUL MCSS	Bogdan Andreea	02.03 2026				
3	COMPARTIMENT STATISTICA	Podina Simona	02.03 2026				
4	COMPARTIMENT IAAM	Dr. Negruț Sabina	02.03 2026				
5	SECTIA I PSIHIATRIE	Dr. Breilean Gabriela	04.03 2026				
6	SECTIAS II PSIHIATRIE	Dr. Luțai Roxana	04.03 2026				
7	SECTIA III PSIHIATRIE	Dr. Negru Dana	04.03 2026				
8	SECTIA IV PSIHIATRIE	Dr. Baboș Daniela	04.03 2026				
9	SECTIA V PSIHIATRIE	Dr. Popa Daniela	04.03 2026				
10	SECTIA VI PSIHIATRIE	Dr. Popescu Ioana	04.03 2026				
11	SECTIA VII PSIHIATRIE	Dr. Bica Antonela	04.03 2026				
12	CABINET ASISTENTA SOCIALA	As. soc. Marușca Daniela	03.03 2026				
13	CABINET MEDICINA INTERNA	Dr. Coceala Nicolae Aurelian	02.03 2026				
14	LAM	Dr. Slovenski Constantina	02.03 2026				
15	FARMACIE	Farm.Rosca Tabita	04.03 2026				
16	STOMATOLOGIE	Dr. Tinca Daniel					
17	ERGOTERAPIE	Iorgovan Carmen	03.03 2026				
18	SERVICIUL CONTABILITATE	Ec.Albeanu Gelu	02.03 2026				

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

19	SERVICIU RUNOS	Ec.Cacuci Adriana	03.03 2026				
20	SERVICIUL ADMINISTRATIV	Ing.Serban Ionel	02.03 2026				
21	COMPARTIMENT JURIDIC	CLARIU ALEXANDRU.	04.03 2026				

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

12. Diagrama de proces

12.1 Procedura

Pas	Responsabil(i)	Descriere	Timp alocat*	Termen**	Riscuri
I. Identificarea activităților de prelucrare					
1.	Responsabil protecția datelor (DPO); Șefi secții/compartimente; RUNOS; Compartiment IT	identificarea categoriilor de date prelucrate la nivelul structurilor spitalului;			Evidență incompletă a activităților de prelucrare (ROPA incomplet)
2.		completarea/actualizarea Registrului activităților de prelucrare (ROPA).			
II. Colectarea datelor cu caracter personal					
3.	Personal medico-sanitar;	la internare;			Colectarea excesivă sau nejustificată de date cu caracter personal
4.	Registratori	în relația de muncă;			
5.	medicali;	prin sisteme informatice sau documente fizice;			
6.	RUNOS; Personal administrativ	prin solicitări ale persoanelor vizate.			
III. Informarea persoanei vizate					
7.	Personal recepție/registratură; RUNOS; Personal medical;	furnizarea notelor de informare GDPR;			Informare incompletă sau neconformă GDPR a persoanei vizate
8.		obținerea consimțământului atunci când este necesar.			

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

Pas	Responsabil(i)	Descriere	Timp alocat*	Termen**	Riscuri
	DPO (suport metodologic)				
IV. Înregistrarea și stocarea datelor					
9.	Compartiment IT;	introducerea în sistemele informatice;			Acces neautorizat la date din cauza configurării incorecte a accesului
10.	Registratori	arhivarea documentelor fizice;			
11.	medicali;				
12.	RUNOS; Personal autorizat	stabilirea drepturilor de acces.			
V. Prelucrarea datelor					
13.	Personal medical;	utilizare exclusiv în scop medical, administrativ sau legal;			Utilizarea datelor în alte scopuri decât cele declaratate
14.	Personal administrativ; Utilizatori autorizați ai sistemelor informatice	acces limitat pe bază de rol.			
VI. Implementarea măsurilor de securitate					
15.	Compartiment IT;	autentificare utilizatori;			Vulnerabilități tehnice care permit acces neautorizat la date
16.	Conducerea	control acces;			
17.	unității; DPO (monitorizare); Furnizori IT	backup;			
		protecție fizică și logică.			
VII. Exercițarea drepturilor persoanelor vizate					
19.	DPO;	primire cerere;			Depășirea termenului legal de răspuns la
20.	Registratură;	identificare solicitant;			

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM	Ediția: 1
	Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Revizia: 0
		Exemplar nr.1

r'as	Responsabil(i)	Descriere	Timp alocat*	Termen**	Riscuri
21.	RUNOS;	analiză DPO;			cererile persoanelor vizate
22.	Structura deținătoare a datelor	formulare răspuns.			
VIII. Gestionarea incidentelor de securitate					
23.	DPO;	notificare internă;			Neraportarea la timp a unui incident de securitate
24.	Compartiment IT;	analiză DPO;			
25.	Conducerea spitalului; Personal raportor	notificare ANSPDCP dacă este cazul.			
IX. Monitorizare și instruire periodică					
26.	DPO; Comisia	instruiri GDPR;			Nivel scăzut de conștientizare GDPR al personalului
27.	SCIM; SMCSS;	auditori interne;			
28.	Conducerea unității	revizuirea procedurii.			

*Timpul alocat operațiunii este stabilit în funcție de complexitatea activității.

** Termenul pentru realizarea operațiunii se stabilește în funcție de complexitatea activității.

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

12.2. Documente utilizate

12.2.1. Lista și proveniența documentelor utilizate

Regulamentul (UE) 2016/679 (GDPR);

- Legea nr. 190/2018;
- Legea nr. 95/2006 privind reforma în domeniul sănătății;
- Proceduri interne ale spitalului privind comunicarea, arhivarea și securitatea informațiilor;
- Registrul activităților de prelucrare a datelor (ROPA);
- Formulare privind exercitarea drepturilor persoanelor vizate;
- Note de informare pacienți/angajați;
- Acorduri de confidențialitate;
- Registrul cererilor persoanelor vizate;
- Registrul incidentelor de securitate;
- Decizii manageriale privind accesul la date și desemnarea responsabililor.

12.2.2. Conținutul și rolul documentelor utilizate

- **ROPA** — evidențiază toate activitățile de prelucrare desfășurate la nivelul spitalului;
- **Notele de informare** — asigură transparența prelucrării față de persoanele vizate;
- **Formular cerere persoană vizată** — permite exercitarea drepturilor GDPR;
- **Registrul cererilor** — asigură trasabilitatea solicitărilor;
- **Acordul de confidențialitate** — stabilește obligațiile personalului;
- **Registrul incidentelor** — documentează încălcările securității datelor;
- **Procedura GDPR** — stabilește cadrul operațional și responsabilitățile.

12.2.3. Circuitul documentelor

- Documentele sunt generate la nivelul compartimentelor funcționale.
- Sunt transmise către DPO pentru analiză/verificare, după caz.
- Sunt aprobate de conducerea spitalului atunci când este necesar.
- Sunt înregistrate în registrele specifice.
- Sunt arhivate:
 - electronic pe serverul instituției;
 - fizic în arhiva unității.
- Accesul este permis doar persoanelor autorizate.

12.3. Resurse necesare

12.3.1. Resurse materiale

Resursele materiale necesare sunt:

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

- calculatoare și terminale informatice securizate;
- servere și infrastructură IT;
- aplicații informatice medicale și administrative;
- spații de arhivare securizate;
- dulapuri metalice încuiate;
- echipamente de backup și protecție antivirus;
- rechizite și formulare specifice.

12.3.2. Resurse umane

Resursele umane necesare sunt:

- Managerul unității sanitare;
- Responsabilul cu protecția datelor (DPO);
- Comisia de monitorizare SCIM;
- Compartiment IT;
- Serviciul RUNOS;
- personal medico-sanitar;
- personal administrativ;
- personal autorizat cu drept de acces la date.

12.3.3. Resurse financiare

Resursele financiare necesare sunt stabilite prin bugetul entității publice și includ:

- cheltuieli pentru infrastructură IT;
- licențe software;
- servicii de mentenanță și securitate informatică;
- instruirea personalului;
- servicii de consultanță și audit în domeniul protecției datelor.

12.4. Modul de lucru

Verificarea rezultatelor activității

Indicatori de performanță

Indicatori de monitorizare a rezultatelor	Analiza rezultatelor dupa implementare			
	Analiza 1 (data)	Analiza 2 (data)	Analiza 3 (data)	Analiza 4 (data)
1. Număr de reclamații privind modul de prelucrare a datelor cu caracter personal/total reclamații la nivel de spital/lună/semestru/an;				

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

2. Număr de încălcări ale securității datelor cu caracter personal justificate / total încălcări ale securității / an.				
--	--	--	--	--

Tabel luare la cunoștință/ instruire de către/ a personalului pentru

Data:

Nr. Crt.	Nume si Prenume	Funcția	Semnătura
1			
2			
3			
4			
5			

Tabel testare personal

Data testării :		Persoana care a efectuat testarea			
Nr. Crt	Nume si Prenume	B.	S.	Ns.	Semnătura
1					
2					
3					
4					

12.5. Anexe, înregistrări, arhivări

- Anexa 1 - Registrul general de evidență al activităților de prelucrare SPMS JEBEL
- Anexa 2 - Notă de informare privind prelucrarea datelor cu caracter personal ale pacienților SPMS Jebel
- Anexa 3 - Notificare generală angajați privind prelucrarea datelor cu caracter personal
- Anexa 4 - Notificare generala candidati privind prelucrarea datelor cu caracter personal
- Anexa 5 - Infografice SPMS JEBEL
- Anexa 6 - Acord privind prelucrarea datelor cu caracter personal
- Anexa 7 - Formular Cerere persoana vizata
- Anexa 8 - Registrul privind cererile persoanelor vizate
- Anexa 9 - Informare asupra obligațiilor angajaților în desfășurarea activităților de prelucrare a datelor cu caracter personal
- Anexa 10 - Acord de confidențialitate GDPR

SPITALUL DE PSIHIATRIE SI PENTRU MASURI DE SIGURANTA JEBEL 	PROCEDURĂ DE SISTEM Privind PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL	Ediția: 1
		Revizia: 0
		Exemplar nr.1

- Anexa 11 - Descrierea postului DPO
- Anexa 12 - Registru măsuri în cazul unei încălcări a securității datelor cu caracter personal
- Anexa 13 - Registru incidente de Securitate
- Anexa 14 - Recomandari întocmire Registru incidente de Securitate
- Anexa 15 - Diagramă care prezintă cerințele de notificare
- Anexa 16 - Formular de notificare a încălcării securității datelor către persoanele vizate

FORMULAR DE NOTIFICARE A ÎNCĂLCĂRII SECURITĂȚII DATELOR CĂTRE PERSOANELE VIZATE

De la: Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel

Către: [numele și adresa persoanei vizate afectate]

Trimisă prin:

- ☐ Poștă
- ☐ Email
- ☐ Fax
- ☐ Altele.....

1. Stimate/stimată domn/doamnă, vă informăm cu regret că la data deam constatat că am suferit o încălcare a securității datelor cu caracter personal.

2. În urma încălcării susmenționate a securității datelor cu caracter personal, este posibil ca datele cu caracter personal care se referă la dumneavoastră să fi fost:

- ☐ divulgate
- ☐ distruse
- ☐ pierdute
- ☐ modificate
- ☐ accesate
- ☐ altele [vă rugăm să specificați alte posibile rezultate]

de persoane neautorizate.

3. Vă rugăm să rețineți că încălcarea securității datelor cu caracter personal ar putea avea următoarele consecințe:

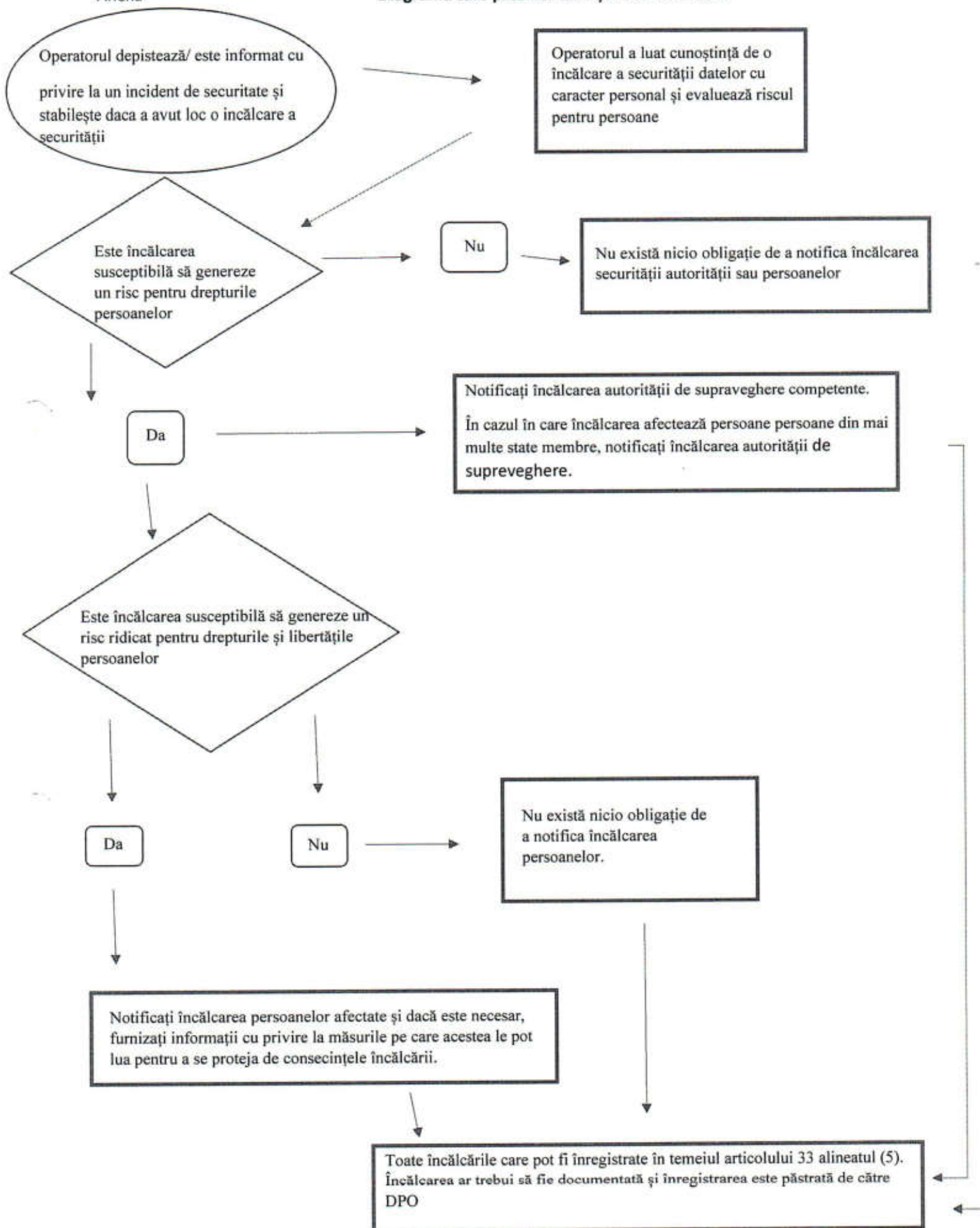
[enumerați toate consecințele posibile]

4. Au fost luate/vor fi luate următoarele măsuri pentru a soluționa încălcarea securității datelor:
[enumerați toate măsurile luate]

5. Dacă aveți întrebări sau îngrijorări legate de încălcarea securității datelor, vă încurajăm să contactați Responsabilul nostru cu protecția datelor, pe adresa de email dpo@spitaljebel.ro sau la adresa: Jebel, Jud. Timiș, Cod postal 307235, România .

Anexă

Diagramă care prezintă cerințele de notificare



afectate și datele altor persoane fizice			
Registrele medicale ale unui spital sunt indisponibile timp de 30 h din cauza unui atac cibernetic.	DA, este necesară notificarea întrucât există un risc ridicat asupra bunăstării pacienților și confidențialității datelor acestora.	DA, este necesară notificarea persoanelor fizice afectate.	
Un mesaj este trimis prin e-mail către destinatari prin folosirea câmpului „către” sau „cc”, ceea ce face posibil ca fiecare destinatar să vadă adresa de e-mail a celorlalți destinatari.	DA, notificarea poate fi necesară în cazul în care un număr mare de persoane fizice sunt afectate, dacă sunt afectate date cu caracter sensibil (de exemplu, o listă de e-mailuri ce aparțin unui medic) sau dacă sunt prezenți alți factori de risc (mesajul trimis prin e-mail ar putea conține parole).	DA, în dependență de tipul de date, scopul colectării și gravitatea consecințelor.	Notificarea incidentului ar putea să nu fie necesară dacă nu sunt dezvăluite date sensibile și dacă un număr infim de e-mailuri au fost dezvăluite.

Exemplu	Necesitatea de a notifica Autoritatea	Necesitatea de a notifica persoana vizată	Note/Recomandări
Operatorul a stocat o copie a unei arhive de date cu caracter personal criptată pe un CD. Acest CD a fost furat.	NU	NU	Atât timp cât datele cu caracter personal sunt criptate cu folosirea unui algoritm, copia există iar cheia de decriptare nu a fost descoperită, acest tip de incident nu necesită o raportare. Totuși, în cazul în care este descoperită cheia, va fi necesară o notificare.
Datele cu caracter personal ale persoanelor fizice au fost extrase de pe o pagină web securizată administrată de către operator în cursul unui atac cibernetice.	DA, în cazul în care există probabilitatea de a surveni consecințe ce ar afecta persoanele fizice.	DA, în dependență de natura datelor cu caracter personal afectate și dacă gradul de risc al consecințelor este unul ridicat.	În cazul în care riscul nu este unul ridicat, se recomandă notificarea persoanelor vizate în dependență de circumstanțele cazului
Operatorul este atacat cu un soft de tip ransomware ce duce la criptarea tuturor datelor. Nu există copii de rezervă iar datele nu pot fi restabilite. În cursul investigației incidentului se descoperă faptul că unicul scop al softului de tip ransomware a fost criptarea datelor fără a le aduce o altfel de atingere.	DA, întrucât acest caz reprezintă o lipsă a disponibilității.	DA, în dependență de natura datelor cu caracter personal afectate și lipsa de disponibilitate, precum și alte posibile consecințe.	În cazul în care exista o copie de rezervă și datele puteau fi recuperate în timp util, acest tip de incident nu necesită a fi raportat către Autoritate și persoanelor vizate întrucât nu genera riscul de a avea o pierdere permanentă a disponibilității sau confidențialității datelor. Totuși, Autoritatea de Supraveghere poate desfășura o investigație pentru a evalua conformitatea cu măsuri extinse de securitate, conform art. 32 RGPD.
O persoană fizică raportează Operatorului un incident de securitate. Aceasta a primit un document cu datele cu caracter personal ale altei persoane. Operatorul efectuează o scurtă investigație (în timp de 24 h) și stabilește faptul că a avut loc un incident de securitate și identifică dacă acest tip de incident este unul sistematic, existând posibilitatea de a fi	DA	Doar persoanele fizice afectate vor fi notificate dacă există un risc ridicat, și este clar că alte persoane fizice nu sunt afectate.	În cazul în care, în urma unei investigații, este identificat faptul că mai multe persoane fizice sunt afectate, se va face o altă notificare către Autoritate, iar operatorul va lua măsuri pentru a notifica și alte persoane fizice dacă există un risc ridicat.

Recomandări întocmire Registru incidente de securitate

MODEL

Registru incidentelor de securitate

Fundamentare:

Potrivit prevederilor art. 33 alin. (5) din Regulamentul General pentru Protecția Datelor, Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acestora și a măsurilor de remediere întreprinse.

Prezentul document propune structura acestui Registru de evidență a încălcărilor de Securitate și cuprinde o listă de exemple non-exhaustive cu scopul de a ajuta Operatorul în luarea deciziei dacă este necesară notificarea incidentelor de securitate în diferite situații.

Nr	Tipul incidentului și modul în care a avut loc acesta	Caracterul încălcării securității datelor	Natura și conținutul datelor afectate de incident	Data și ora descoperirii	Data și ora survenirii	Persoana a care a descoperit incidentul	Persoana responsabilă de domeniul în care a survenit incidentul	Gradul de probabilitate privind afectarea drepturilor persoanelor vizate	Măsurile luate anterior pentru prevenirea unui astfel de incident	Măsurile luate pentru a opri incidentul /ameliora situația	Necesitatea de a comunica incidentul Autorității Naționale/Persoanelor vizate	Numărul aproximativ și categoriile persoanelor vizate afectate	Consecințele probabile ale incidentului
----	---	---	---	--------------------------	------------------------	---	---	--	---	--	---	--	---

*Notă

- ✓ Coloana *tipul incidentului și modul în care a avut loc acesta* se va completa cu termeni precum: distrugere, pierdere, modificare, divulgare neautorizată, acces neautorizat etc; prin e-mail, în mod fizic etc.
- ✓ Coloana *caracterul încălcării securității datelor* se va completa cu termeni precum: confidențialitate, integritate, disponibilitate.
- ✓ Coloana *persoana care a descoperit incidentul și persoana responsabilă de domeniul în care a survenit incidentul* se va completa prin indicarea numelui, prenumelui și funcției persoanei.
- ✓ Coloana *gradul de probabilitate privind afectarea drepturilor persoanelor vizate* se va completa prin indicarea unuia dintre următoarele grade: inexistent, infim, mic, mediu, ridicat, absolut. Gradul de probabilitate se va stabili de către Comisia care va analiza incidentul de securitate.
- ✓ Coloana *necesitatea de a comunica incidentul Autorității Naționale/Persoanelor vizate* se va completa prin indicarea răspunsurilor după modelul: DA/NU, DA/DA, NU/NU.
- ✓ Coloana *numărul aproximativ și categoriile persoanelor vizate afectate* se va completa în ceea ce privește categoria persoanelor vizate prin folosirea noțiunilor precum: minori, angajați, cetățeni, pacienți, clienți, copii etc.

Mai jos este prezentată o listă de exemple non-exhaustive, conform Orientărilor privind notificarea incidentelor de securitate ce au scopul de a ajuta operatorul în luarea deciziei dacă este necesară notificarea incidentelor de securitate în diferite situații. Aceste exemple, de asemenea, pot contribui la diferențierea gradului de risc asupra drepturilor și libertăților persoanelor vizate.

Registru măsuri în cazul unei încălcări a securității

[illegible]

- să coopereze cu autoritatea pentru protecția datelor și să reprezinte punctul de contact în relația cu aceasta.

Baza legală privind funcția Responsabilului pentru protecția datelor, o reprezintă art. 38 alin.3 din Regulament care stabilește câteva condiții, respectiv:

- Responsabilul cu protecția datelor nu primește nici un fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor sale de la operator sau de la persoana împuternicită de operator;
- Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

VII. DATELE DE CONTACT ALE RESPONSABILULUI PENTRU PROTECȚIA DATELOR

DPO Extern : SC DAF Consulting & Management SRL

email : dpo@dafcons.ro

telefon : 0724.617.735

Persoana de contact : Responsabil cu protecția datelor – Dl. Dragoș Tecioiu

email : dragos.tecioiu@dafcons.ro

telefon: 0723.141.821



www.SpitalJebel.ro

MINISTERUL SĂNĂTĂȚII
Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel
Adresă: Localitatea Jebel, Cod postal 307185, România
TEL: 0256/394442 ; 0256/394443
FAX: 0256/394021 ; 0256/394026
email : secretariat@spitaljebel.ro

RESPONSABILUL CU PROTECȚIA DATELOR CU CARACTER PERSONAL

NUMIREA ȘI DESCRIEREA POSTULUI

Prezentul document conține descrierea postului de responsabil cu protecția datelor cu caracter personal astfel cum această poziție este reglementată prin 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 și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

Prezentul document are drept scop informarea completă a angajaților SPMS JEBEL cu privire la rolul și poziția responsabilului cu protecția datelor în cadrul instituției și va fi modificat și completat ori de câte ori legislația în domeniul protecției datelor cu caracter personal va suferi modificări sau completări.

La redactarea prezentului document au fost utilizate și resursele informaționale furnizate de "Ghidul privind responsabilul cu protecția datelor" al Grupului de Lucru pentru art. 29 ("GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL"), revizuit și adoptat la Bruxelles la data de 05.04.2017.

I. CONCEPTUALIZAREA SUBIECTULUI

Regulamentul General privind protecția datelor (GDPR) aplicabil din data de 25 mai 2018 în toate statele membre ale Uniunii Europene, instituie un cadru legal de conformitate în vederea aplicării unitare a principiilor și regulilor de prelucrare a datelor cu caracter personal în Europa, conținând pe lângă elementele clasice ale conceptului de protecție a datelor personale și elemente de noutate menite să asigure responsabilizarea operatorilor de date cu caracter personal.

În acest context, responsabilul cu protecția datelor cu caracter personal ocupă o poziție centrală în noul cadru juridic privind protecția datelor cu caracter personal.

Potrivit GDPR este obligatorie numirea unui responsabil cu protecția datelor cu caracter personal în cadrul **tuturor autorităților și organismelor publice indiferent de tipul datelor cu caracter personal prelucrate.**

În viziunea GDPR, responsabilul cu protecția datelor cu caracter personal reprezintă un important punct de responsabilizare pentru că, adiacent activității de facilitare a respectării prevederilor GDPR, (de ex. facilitarea evaluărilor impactului asupra protecției datelor și efectuarea sau facilitarea auditurilor), responsabilul cu protecția datelor cu caracter personal acționează și ca intermediar între părțile interesate (spre exemplu autoritatea de supraveghere, persoanele vizate și operator).

Respectarea normelor de protecție a datelor continuă să rămână responsabilitatea operatorului, care are un rol crucial cu privire la îndeplinirea eficientă a atribuțiilor responsabilului cu protecția datelor. Numirea unei astfel de persoane reprezintă pentru operator un prim pas în vederea conformării însă operatorului îi revine sarcina de a se asigura ca responsabilul cu protecția datelor are autonomie și resurse suficiente pentru îndeplinirea sarcinilor sale în mod eficient.

II. NUMIREA RESPONSABILULUI CU PROTECȚIA DATELOR CU CARACTER PERSONAL

- **Expertiza responsabilului cu protecția datelor cu caracter personal**

Articolul 37 alin. 5 din GDPR prevede că responsabilul cu protecția datelor cu caracter personal „este desemnat pe baza calităților profesionale și, **în special, a cunoștințelor de specialitate în dreptul și practicile în domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la art. 39 (articol ce prevede atribuțiile)”. Nivelul necesar al cunoștințelor de specialitate a responsabilului cu protecția datelor trebuie să fie stabilit în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate.**

- **Capacitatea de îndeplinire a sarcinilor responsabilului cu protecția datelor cu caracter personal**

Responsabilul cu protecția datelor trebuie să poată face dovada calităților personale prin care să respecte integritatea și etica profesională având ca principală preocupare respectarea GDPR.

Capacitățile responsabilului cu protecția datelor cu caracter personal trebuie să îi confere posibilitatea de a juca un rol –cheie în promovarea unei culturi de protecție a datelor și de a oferi suport în implementarea elementelor esențiale ale GDPR de ex: principiile de prelucrare a datelor, drepturile persoanelor vizate, asigurarea protecției

datelor începând cu momentul conceperii și în mod implicit înregistrarea activităților de prelucrare, securitatea prelucrării precum și notificarea și comunicarea încălcărilor de securitate.

III. POZIȚIA RESPONSABILULUI CU PROTECȚIA DATELOR CU CARACTER PERSONAL

- **Implicarea responsabilului cu protecția datelor cu caracter personal**

Obligația operatorului stabilită prin GDPR (art. 38) este aceea de a implica responsabilul cu protecția datelor cu caracter personal în toate aspectele legate de protecția datelor în mod corespunzător și în timp util. Prin obligația instituită în sarcina operatorului se urmărește astfel ca responsabilul cu protecția datelor și echipa sa să fie implicat cât mai rapid posibil în toate aspectele legate de protecția datelor. În ceea ce privește evaluările impactului asupra protecției datelor, GDPR prevede în mod expres implicarea responsabilului cu protecția datelor și precizează că operatorul solicită avizul responsabilului cu protecția datelor atunci când se efectuează o astfel de evaluare a impactului.

GDPR urmărește ca prin implicarea la timp a responsabilului cu protecția datelor să se faciliteze instituției respectarea cerințelor legale în materie de prelucrare a datelor. Responsabilul cu protecția datelor este astfel văzut ca un partener de discuție în cadrul instituției și ar trebui să facă parte din grupurile de lucru relevante care se ocupă cu activități de prelucrare a datelor.

IV. PUBLICAREA DATELOR DE CONTACT ALE RESPONSABILULUI CU PROTECȚIA DATELOR CU CARACTER PERSONAL

SPMS JEBEL are obligația în temeiul art. 37 alin 7. GDPR:

- (i) Să publice datele de contact ale responsabilului cu protecția datelor
- (ii) Să comunice datele de contact ale responsabilului cu protecția datelor autorității de supraveghere

SPMS JEBEL se asigură că aceste obligații sunt îndeplinite întocmai pentru a se asigura că persoanele vizate (atât cele din interiorul instituției cât și cele din exterior) dar și autoritatea de supraveghere pot contacta cu ușurință responsabilul cu protecția datelor cu caracter personal fără a fi necesar să intervină o altă parte. În acest sens SPMS JEBEL facilitează persoanelor vizate și autorității de supraveghere căi adecvate de comunicare cu

responsabilul pentru protecția datelor cu caracter personal și asigură confidențialitatea acestor comunicări.

V. RESURSELE NECESARE RESPONSABILULUI CU PROTECȚIA DATELOR CU CARACTER PERSONAL

SPMS JEBEL are obligația în temeiul dispozițiilor art. 38 alin 2 GDPR să asigure responsabilului cu protecția datelor cu caracter personal:

- (i) Sprijin activ din partea managementului superior
- (ii) Timp suficient pentru îndeplinirea atribuțiilor
- (iii) Sprijin corespunzător în ceea ce privește resursele financiare, infrastructură
- (iv) Comunicare oficială către toți angajații cu privire la numirea responsabilului cu protecția datelor cu caracter personal astfel încât să fie cunoscută prezența sa în cadrul Instituției
- (v) Accesul necesar la expertiza departamentelor/serviciilor precum: resurse umane, achiziții publice, juridic, IT etc astfel încât să beneficieze de sprijin activ și esențial, reacții și informații
- (vi) Resurse pentru pregătirea continuă în domeniul protecției datelor cu caracter personal

VI. ATRIBUȚIILE RESPONSABILULUI CU PROTECȚIA DATELOR

Responsabilul cu protecția datelor cu caracter personal exercită o misiune de consiliere, informare și de control fiind punctul de legătura între operator și autoritatea de supraveghere a prelucrării datelor cu caracter personal.

Potrivit dispozițiilor GDPR (art. 38,39) rolul responsabilului cu protecția datelor este:

- să informeze și să consilieze SPMS JEBEL sau persoana împuternicită, precum și angajații, cu privire la obligațiile existente în domeniul protecției datelor cu caracter personal.
- să monitorizeze respectarea regulamentului și a legislației naționale în domeniul protecției datelor, să consilieze SPMS JEBEL sau persoana împuternicită în legătură cu realizarea de studii de impact privind protecția datelor și să verifice efectuarea acestora.



www.SpitalJebel.ro

MINISTERUL SĂNĂTĂȚII
Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel
Adresa: Localitatea Jebel, Cod postal 307235, România
TEL: 0256/394442 ; 0256/394443
FAX: 0256/394021 ; 0256/394026
email : secretariat@spitaljebel.ro

ACORD DE CONFIDENȚIALITATE

Confirm faptul că:

- a) am luat la cunoștință obligațiile angajaților în desfășurarea activităților de prelucrarea a datelor cu caracter personal ;
- b) am fost informat și instruit conform prevederilor Regulamentului general privind protecția datelor cu caracter personal.

Înțeleg că am obligația de a respecta dispozițiile privind prelucrarea datelor cu caracter personal menționate în **Informarea asupra obligațiilor angajaților în desfășurarea activităților de prelucrare a datelor cu caracter personal** în considerarea calității mele de salariat al Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel.

Îmi asum personal responsabilitatea pentru respectarea integrală a principiilor, cerințelor și obligațiilor menționate în Informarea asupra obligațiilor angajaților în desfășurarea activităților de prelucrare a datelor cu caracter personal în cadrul Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel.

Subsemnatul/subsemnata:

..... ,
Data nașterii: __/__/__, angajat/ă în Funcția/Postul

Departamentul/Serviciul.....

Biroul.....

Data :

Semnătura :



www.SpitalJebel.ro

MINISTERUL SĂNĂTĂȚII

Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel

Adresa: Localitatea Jebel, Cod postal 307235, România

TEL: 0256/394442 ; 0256/394443

FAX:0256/394021 ; 0256/394026

email : secretariat@spitaljebel.ro

Salariatul are obligația de a păstra confidențialitatea asupra datelor personale pe care le prelucrează pe toată durata contractului pe care acesta l-a încheiat cu Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel, dar și după încetarea acestuia, pe termen nelimitat.



www.SpitalJebel.ro



MINISTERUL SĂNĂTĂȚII
Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel
Adresa: Localitatea Jebel, Cod postal 307235, România
TEL: 0256/394442 ; 0256/394443
FAX: 0256/394021 ; 0256/394026
email : secretariat@spitaljebel.ro

INFORMARE ASUPRA OBLIGAȚIILOR ANGAJAȚILOR ÎN DESFĂȘURAREA ACTIVITĂȚILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

În conformitate cu Regulamentul (UE) 2016/679 (GDPR) privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, personalul angajat al Spitalului de Psihiatrie și pentru Măsuri de Siguranță Jebel are obligația:

- a) de a prelucra datele cu caracter personal în conformitate cu și în limitele de autorizare stabilite în procedurile interne ale angajatorului;
- b) de a păstra confidențialitatea asupra datelor personale pe care le prelucrează;
- c) de a nu dezvălui datele personale pe care le prelucrează unor alte persoane decât cele în viza cărora îi este permis acest lucru prin procedurile interne, prin Procedura de Sistem privind protecția datelor cu caracter personal, prin regulamentul intern al angajatorului, fișa postului și prin contractul individual de muncă, contractul de colaborare sau orice alt tip de contract semnat între părți;
- d) de a prelucra datele personale numai pentru aducerea la îndeplinire a atribuțiilor de serviciu prevăzute în regulamentul intern, în fișa postului, în contractul individual de muncă sau orice alt tip de contract semnat între părți;
- e) de a respecta măsurile tehnice și organizatorice stabilite pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmiterea de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală;
- f) de a nu utiliza date cu caracter personal în scopuri personale sau comerciale;
- g) de a aduce la cunoștință angajatorului în cel mai scurt timp posibil orice situație de acces neautorizat la datele personale pe care le prelucrează.

Nerespectarea obligațiilor prevăzute anterior atrage răspunderea disciplinară a salariatului în conformitate cu prevederile regulamentului intern până la și inclusiv încetarea raportului de muncă.



www.SpitalJebel.ro

MINISTERUL SĂNĂTĂȚII

Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel

Adresa: Localitatea Jebel, Cod postal 307235, România

TEL: 0256/394442 ; 0256/394443

FAX: 0256/394021 ; 0256/394026

email : secretariat@spitaljebel.ro

După completare, vă rugăm să depuneți acest formular, personal, pe baza actului de identitate, la adresa : Jebel, Jud. Timiș, Cod postal 307235, România sau să o trimiteți pe adresa de email dpo@spitaljebel.ro.



www.SpitalJebel.ro



MINISTERUL SĂNĂTĂȚII
Spitalul de Psihiatrie și pentru Măsurile de Siguranță Jebel
Adresa: Localitatea Jebel, Cod postal 307235, România
TEL: 0256/394442 ; 0256/394443
FAX: 0256/394021 ; 0256/394026
email : secretariat@spitaljebel.ro

FORMULAR CERERE PERSOANĂ VIZATĂ

(pentru exercitarea drepturilor prevăzute la art. 12-22, 34 din GDPR)

Detalii privind persoana vizată (titularul cererii):

Nume, Prenume:

Modalitate de contact (adresă de e-mail sau adresă poștală):

Obiectul cererii:

Vă rugăm să selectați care este obiectul cererii dumneavoastră:

- ☐ Retragere a consimțământului pentru prelucrarea de date cu caracter personal;
- ☐ Cerere de acces la datele cu caracter personal;
- ☐ Cerere de rectificare a datelor cu caracter personal;
- ☐ Cerere de ștergere a datelor cu caracter personal;
- ☐ Cerere de restricționare a prelucrării datelor cu caracter personal;
- ☐ Cerere de portare a datelor cu caracter personal;
- ☐ Cerere de opoziție la prelucrarea datelor cu caracter personal;
- ☐ Cerere privind prelucrările automate și crearea de profile.

Categoriile de date cu caracter personal care fac obiectul cererii:

Detalii privind cererea dumneavoastră:

Data: / /

Semnătura:



www.SpitalJebel.ro



MINISTERUL SĂNĂTĂȚII
Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel
Adresa: Localitatea Jebel, Cod postal 307235, România
TEL: 0256/394442 ; 0256/394443
FAX:0256/394021 ; 0256/394026
email : secretariat@spitaljebel.ro

ACORD

privind prelucrarea datelor cu caracter personal

Subsemnatul/Subsemnata,, identificat(ă) cu
BI/CI seria, nr., domiciliat în Str., nr.,
Bloc, Scara, Ap., localitate, județ/sector

Prin prezentul acord îmi exprim în mod expres consimțământul SPMS JEBEL să prelucreze datele mele cu
caracter personal care sunt oferite de către mine, cu scopul de

.....

.....

Nume, Prenume:

Data :/...../.....

Semnătura:

Confirm că mi s-au adus la cunoștință drepturile mele prevăzute de Regulamentul General de Protecție a
Datelor cu Caracter Personal nr.679/2016 și că am luat la cunoștință de INFORMAREA PRIVIND
PRELUCRAREA DATELOR CU CARACTER PERSONAL în cadrul SPMS JEBEL.

Nume, Prenume:

Data :/...../.....

Semnătura:

Prezentul acord a fost întocmit în două exemplare, un exemplar pentru declarant și un exemplar pentru
spital.

INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL A PACIENȚILOR

SPITALUL DE PSIHIATRIE ȘI PENTRU MĂSURI DE SIGURANȚĂ
JEBEL



DE CE AVEM NEVOIE DE DATELE DUMNEAVOASTRĂ?

Colectăm date despre dumneavoastră pentru identificare și pentru a vă putea oferi acces la servicii medicale, conform nevoilor dumneavoastră.

Colectarea, prelucrarea și stocarea datelor personale utilizate în cadrul prestării serviciilor medicale se desfășoară în baza prevederilor legale specifice din domeniul sănătății.

TIPURI DE DATE COLECTATE



Date de identificare, date de contact, date despre starea de sănătate, date financiare.

Categoriile speciale de date, cum sunt datele despre starea dumneavoastră de sănătate, sunt prelucrate conform derogărilor prevăzute în art. 9.2(h) și 9.2 (i) din Regulamentul General pentru Protecția Datelor nr. 679 din 27.04.2016.



SCOPUL PRELUCRĂRII ȘI TEMEIUL LEGAL

Datele dumneavoastră sunt prelucrate de către instituția noastră în scopul îndeplinirii atribuțiilor legale ce ne revin conform legii, respectiv în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente medicale pentru pacient ori de gestionare a serviciilor de sănătate care acționează în interesul pacientului.

ESTE POSIBIL SĂ TRANSFERĂM DATELE DUMNEAVOASTRĂ



Către autorități competente, când prevederile legale ne impun acest lucru: Casa de Asigurări de Sănătate - C.A.S., Direcția de Sănătate Publică - D.S.P., Dosarul Electronic de Sănătate - D.E.S., Autoritatea Națională de Management al Calității în Sănătate - A.N.M.C.S., Inspectoratul Teritorial de Muncă - I.T.M., Agenția Națională de Administrare Fiscală, etc.



TRANSFER INTERNAȚIONAL

Datele cu caracter personal furnizate către SPMS JEBEL nu sunt transferate în afara Spațiului Economic European.

PERIOADA DE STOCARE A DATELOR



Datele cu caracter personal vor fi păstrate atât timp cât este necesar pentru scopurile menționate mai sus cu respectarea în același timp a cerințelor legale în vigoare și a interesului de protejare a drepturilor persoanelor vizate.



DREPTURILE DE CARE BENEFICIAȚI

În conformitate cu prevederile GDPR, vă puteți exercita următoarele drepturi în legătură cu datele dumneavoastră cu caracter personal: dreptul de acces, dreptul de a solicita rectificarea și actualizarea datelor, și, în anumite circumstanțe, dreptul de a solicita restricționarea prelucrării, dreptul de opoziție, dreptul de a fi uitat, dreptul de portabilitate a datelor. Aveți de asemenea, dreptul de a depune plângere în fața Autorității de Supraveghere și dreptul de a vă adresa justiției.

INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIN INTERMEDIUL SISTEMELOR DE SUPRAVEGHERE VIDEO

SPITALUL DE PSIHIATRIE ȘI PENTRU MĂSURI DE SIGURANȚĂ JEBEL



Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel prelucrează date cu caracter personal prin intermediul sistemelor video, respectiv imaginea și alte informații ce permit identificarea unei persoane fizice, în scopul monitorizării accesului persoanelor în instituție, al asigurării securității spațiilor și bunurilor instituției, precum și al siguranței persoanelor aflate în sediul instituției.

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

- a) chiar dacă nu sunt asociate cu datele de identificare ale persoanei, sau
- b) chiar dacă nu conțin imaginea persoanei filmate, ci alte informații de natura să conducă la identificarea acesteia (ex: numărul de înmatriculare al vehiculului).



SCOPUL ȘI TEMEIUL LEGAL AL PRELUCRĂRII

Scopul prelucrării datelor cu caracter personal constă în: monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor private, prevenirea și combaterea infracțiunilor, îndeplinirea obligațiilor legale, realizarea intereselor legitime. SPMS Jebel nu va prelucra datele personale în alte scopuri în afara celor menționate mai sus.

Temeiul legal pentru aceasta prelucrare este Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor cu modificările și completările ulterioare, prelucrarea fiind necesară în vederea îndeplinirii unei obligații legale și realizarea intereselor legitime ale operatorului.

PERIOADA DE STOCARE A DATELOR



Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video este de maxim 30 de zile. La expirarea termenului înregistrările se distrug sau se șterg, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate.



ACCESUL LA DATELE CU CARACTER PERSONAL ȘI DESTINATARIILE ACESTOR DATE

Accesul la datele cu caracter personal este realizat numai de către personalul SPMS Jebel dedicat acestei activități. Aceste date pot fi comunicate persoanelor din afara SPMS Jebel doar atunci când acest lucru este necesar pentru atingerea scopului prelucrării și/sau în cazurile prevăzute de lege.

DREPTURILE DE CARE BENEFICIAȚI



În conformitate cu prevederile GDPR, vă puteți exercita următoarele drepturi în legătură cu datele dumneavoastră cu caracter personal: dreptul de acces, dreptul de a solicita rectificarea și actualizarea datelor, și, în anumite circumstanțe, dreptul de a solicita restricționarea prelucrării, dreptul de opoziție, dreptul de a fi uitat, dreptul de portabilitate a datelor. Aveți de asemenea, dreptul de a depune plângere în fața Autorității de Supraveghere și dreptul de a vă adresa justiției.



www.SpitalJebel.ro



MINISTERUL SĂNĂTĂȚII
Spitalul de Psihiatrie și pentru Măsurile de Siguranță Jebel
Adresa: Localitatea Jebel, Cod postal 307235, România
TEL: 0256/394442 ; 0256/394443
FAX: 0256/394021 ; 0256/394026
email : secretariat@spitaljebel.ro

JEBEL (Art. 6 alin. 1 lit. f din GDPR), și anume monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor private, prevenirea și combaterea infracțiunilor.

SPMS JEBEL colectează date cu caracter personal doar în scopuri determinate, explicite și legitime. Datele colectate sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate, prin urmare SPMS JEBEL nu prelucreză date în afara scopului declarat.

SPMS JEBEL, prin Serviciul Resurse Umane Normare Organizare și Salarizare nu poate iniția demersurile privind înscrierea la concurs în cazul unui refuz din partea persoanei vizate, de a furniza date cu caracter personal.

III. CUM SE COLECTEAZĂ DATELE CU CARACTER PERSONAL

SPMS JEBEL colectează datele cu caracter personal:

- în mod direct de la dumneavoastră, în calitate de persoană vizată.
- indirect prin intermediul sistemelor de monitorizare video, sau de la terțe părți cum ar fi instituții de învățământ, foști angajatori, din surse publice.

IV. PERIOADA DE STOCARE A DATELOR PERSONALE

Datele cu caracter personal vor fi păstrate atât timp cât este necesar pentru scopurile menționate mai sus cu respectarea în același timp a cerințelor legale în vigoare și a interesului de protejare a drepturilor persoanelor vizate.

Datele cu caracter personal sunt prelucrate pe toată durata desfășurării concursului, până la maxim 90 de zile de la validarea rezultatelor, după care, în cazul în care nu veți fi declarat admis pentru ocuparea postului vacant vă vor fi restituite, respectiv șterse/distruse din baza de date. În cazul ocupării postului, datele preluate vor constitui dosarul dumneavoastră de personal, urmând a fi prelucrate în scopul încheierii și executării contractului de muncă. În ceea ce privește perioada de stocare a datelor prelucrate prin intermediul sistemelor de supraveghere video, aceasta este de 30 de zile. La expirarea termenului înregistrările se distrug sau se șterg automat, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate.

V. DREPTURILE DUMNEAVOASTRĂ

Potrivit Regulamentului general de protecție a datelor, aveți următoarele drepturi:

- ✓ Dreptul la informare în cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate direct de la aceasta (Art. 13 GDPR)
- ✓ Dreptul de acces al persoanei vizate la prelucrarea datelor și furnizarea unei copii a datelor procesate (Art. 15 GDPR);
- ✓ Dreptul de a solicita rectificarea datelor inexacte sau completarea datelor incomplete (Art. 16 GDPR);
- ✓ Dreptul de a solicita ștergerea datelor cu caracter personal și, în cazul în care datele cu caracter personal au fost făcute publice, transmiterea informațiilor referitoare la solicitarea de ștergere către alți operatori (Art. 17 GDPR);
- ✓ Dreptul de a solicita restricționarea prelucrării datelor (Art. 18 GDPR);
- ✓ Dreptul de a primi datele personale ale dumneavoastră într-un format structurat, utilizat în mod obișnuit și electronic și de a solicita transmiterea acestor date către un alt operator (Art. 20 GDPR);
- ✓ Dreptul de a vă opune prelucrării datelor cu intenția de a înceta prelucrarea (Art. 21 GDPR);
- ✓ Dreptul de a depune o plângere la autoritatea de supraveghere dacă considerați că prelucrarea datelor este o încălcare a Regulamentului privind protecția datelor cu caracter personal. (Art. 77 GDPR).

Pentru exercitarea drepturilor legale în legătură cu datele dumneavoastră vă puteți adresa responsabilului cu prelucrarea datelor cu caracter personal al SPMS JEBEL la adresa de e-mail dpo@spitaljebel.ro.

VI. AUTORITATEA NAȚIONALĂ DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

În România, autoritatea de supraveghere este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal cu următoarele date de contact:

- ⇒ email: anspdcp@dataprotection.ro
- ⇒ tel: +40.318.059.211/+40.318.059.212
- ⇒ adresă: B-dul G-ral. Gheorghe Magheru nr. 28-30, Sector 1, cod poștal 010336, București.



www.SpitalJebel.ro



MINISTERUL SĂNĂTĂȚII
Spitalul de Psihiatrie și pentru Măsură de Siguranță Jebel
Adresa: Localitatea Jebel, Cod postal 307235, România
TEL: 0256/394442 ; 0256/394443
FAX: 0256/394021 ; 0256/394026
email : secretariat@spitaljebel.ro

NOTIFICARE CU PRIVIRE LA PROTECȚIA DATELOR CU CARACTER PERSONAL

Către: _____

Am primit un exemplar: _____

I. INFORMAȚII GENERALE

Prezenta notificare este redactată în vederea informării cu privire la datele dumneavoastră cu caracter personal precum și cu privire la drepturile pe care le aveți în legătură cu prelucrarea acestor date.

Prelucrarea datelor cu caracter personal se face în conformitate cu prevederile Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor GDPR) precum și cu celelalte legi naționale relevante aplicabile relațiilor de muncă și protecției datelor cu caracter personal.

OPERATORUL:

SPMS JEBEL, cu sediul în Jebel, Jud. Timiș, Cod postal 307235, România, este operator de date cu caracter personal și prin urmare este responsabil pentru protecția datelor descrisă mai jos. Pentru întrebări sau solicitări privind datele cu caracter personal vă rugăm să contactați ofițerul nostru pentru protecția datelor cu caracter personal la datele indicate în prezenta.

RESPONSABILUL DE DATE CU CARACTER PERSONAL:

Puteți contacta ofițerul nostru pentru protecția datelor cu caracter personal prin email la: dpo@spitaljebel.ro.

II. PRELUCRAREA DATELOR CU CARACTER PERSONAL

SPMS JEBEL prelucrează datele dumneavoastră personale în conformitate cu prevederile Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, ale legilor naționale și europene privind protecția datelor precum și, în calitate de angajator, în conformitate cu prevederile specifice legislației muncii.

SPMS JEBEL va solicita date cu caracter personal în vederea recrutării personalului pentru stabilirea aptitudinilor necesare și pentru evaluarea experienței profesionale a acestora pentru postul/ poziția pentru care se recrutează. În acest sens Serviciul Resurse Umane Normare Organizare și Salarizare, solicită un set de documente pe baza cărora se realizează prelucrarea datelor cu caracter personal. Datele pot include, dar nu se limitează la:

- Date de identificare, contact, statut: nume, prenume, cod numeric personal, data nașterii, telefon mobil personal, adresa de e-mail, starea civilă, etc.;
- Date privind experiența profesională: CV-uri, scrisoare de recomandare, adeverința vechime etc.;
- Date legate de studii, competențe: diploma de licență, certificat de specialist sau primar, adeverința de malpraxis etc.;
- Date privind starea de sănătate: adeverința de la medicul de familie, certificat medical tip A5, etc.;
- Date despre infracțiuni sau condamnări definitive, acestea fiind solicitate doar cu respectarea prevederilor legale în vigoare.

Prelucrarea datelor cu caracter personal se face având ca temei legal Art. 6 alin. 1 lit. b, și c din Regulamentul general privind protecția datelor (GDPR), respectiv în **vederea executării unui contract sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract și în vederea îndeplinirii obligațiilor legale ce revin instituției.**

Categoriile speciale de date - date despre starea de sănătate a persoanei vizate, necesare în scopuri legate de medicina preventivă sau a muncii, sau pentru evaluarea capacității de muncă a angajatului - sunt prelucrate conform derogărilor prevăzute în art. 9.2(h) din GDPR.

În ceea ce privește înregistrarea prin intermediul sistemelor de supraveghere video interne a imaginilor din spațiile și zonele comune ale instituției, prelucrarea datelor dumneavoastră se **bazează pe interesul legitim al SPMS**



www.SpitalJebel.ro

MINISTERUL SĂNĂTĂȚII

Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel

Adresa: Localitatea Jebel, Cod postal 307235, România

TEL: 0256/394442 ; 0256/394443

FAX:0256/394021 ; 0256/394026

email : secretariat@spitaljebel.ro

⇒ adresă: B-dul G-ral. Gheorghe Magheru nr. 28-30, Sector 1, cod poștal 010336, București.



www.SpitalJebel.ro

MINISTERUL SĂNĂTĂȚII

Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel

Adresa: Localitatea Jebel, Cod postal 307235, România

TEL: 0256/394442 ; 0256/394443

FAX: 0256/394021 ; 0256/394026

email : secretariat@spitaljebel.ro

Categoriile speciale de date - date despre starea de sănătate a persoanei vizate, necesare în scopuri legate de medicina preventivă sau a muncii, pentru evaluarea capacității de muncă a angajatului, diagnostic medical, sănătate sau asistență socială - sunt prelucrate conform derogărilor prevăzute în art. 9.2(h) din GDPR. În ceea ce privește înregistrarea prin intermediul sistemelor de supraveghere video interne a imaginilor din spațiile și zonele comune ale instituției, prelucrarea datelor dumneavoastră se **bazează pe interesul legitim al SPMS JEBEL** (Art. 6 alin. 1 lit. f din GDPR), și anume monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor private, prevenirea și combaterea infracțiunilor.

SPMS JEBEL colectează date cu caracter personal doar în scopuri determinate, explicite și legitime. Datele colectate sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate, prin urmare SPMS JEBEL nu prelucrează date în afara scopului declarat.

SPMS JEBEL, prin Serviciul Resurse Umane Normare Organizare și Salarizare nu poate iniția demersurile privind înscrierea la concurs în cazul unui refuz din partea persoanei vizate, de a furniza date cu caracter personal.

II. CUM SE COLECTEAZĂ DATELE CU CARACTER PERSONAL

SPMS JEBEL colectează datele cu caracter personal:

- în mod direct de la dumneavoastră, în calitate de persoană vizată.
- indirect prin intermediul sistemelor de monitorizare video, sau de la terțe părți cum ar fi instituții de învățământ, foști angajatori, din surse publice.

III. PERIOADA DE STOCARE A DATELOR PERSONALE

Datele cu caracter personal vor fi păstrate atât timp cât este necesar pentru scopurile menționate mai sus cu respectarea în același timp a cerințelor legale în vigoare și a interesului de protejare a drepturilor persoanelor vizate.

IV. DREPTURILE DUMNEAVOASTRĂ

Potrivit Regulamentului general de protecție a datelor, aveți următoarele drepturi:

- ✓ Dreptul la informare în cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate direct de la aceasta (Art. 13 GDPR)
- ✓ Dreptul de acces al persoanei vizate la prelucrarea datelor și furnizarea unei copii a datelor procesate (Art. 15 GDPR);
- ✓ Dreptul de a solicita rectificarea datelor inexacte sau completarea datelor incomplete (Art. 16 GDPR);
- ✓ Dreptul de a solicita ștergerea datelor cu caracter personal și, în cazul în care datele cu caracter personal au fost făcute publice, transmiterea informațiilor referitoare la solicitarea de ștergere către alți operatori (Art. 17 GDPR);
- ✓ Dreptul de a solicita restricționarea prelucrării datelor (Art. 18 GDPR);
- ✓ Dreptul de a primi datele personale ale dumneavoastră într-un format structurat, utilizat în mod obișnuit și electronic și de a solicita transmiterea acestor date către un alt operator (Art. 20 GDPR);
- ✓ Dreptul de a vă opune prelucrării datelor cu intenția de a înceta prelucrarea (Art. 21 GDPR);
- ✓ Dreptul de a depune o plângere la autoritatea de supraveghere dacă considerați că prelucrarea datelor este o încălcare a Regulamentului privind protecția datelor cu caracter personal. (Art. 77 GDPR).

Pentru exercitarea drepturilor legale în legătură cu datele dumneavoastră vă puteți adresa responsabilului cu prelucrarea datelor cu caracter personal al SPMS JEBEL la adresa de e-mail dpo@spitaljebel.ro

V. AUTORITATEA NAȚIONALĂ DE PROTECȚIE A DATELOR CU CARACTER PERSONAL (ANPDPC)

În România, autoritatea de supraveghere este ANPDPC, cu următoarele date de contact:

⇒ email: anspdc@dataprotection.ro

⇒ tel: +40.318.059.211/+40.318.059.212



www.SpitalJebel.ro



MINISTERUL SĂNĂTĂȚII
Spitalul de Psihiatrie și pentru Măsurile de Siguranță Jebel
Adresa: Localitatea Jebel, Cod postal 307235, România
TEL: 0256/394442 ; 0256/394443
FAX: 0256/394021 ; 0256/394026
email : secretariat@spitaljebel.ro

NOTIFICARE CU PRIVIRE LA PROTECȚIA DATELOR CU CARACTER PERSONAL

Către:

Am primit un exemplar:

I. INFORMAȚII GENERALE

Prezenta notificare este redactată în vederea informării cu privire la datele dumneavoastră cu caracter personal precum și cu privire la drepturile pe care le aveți în legătură cu prelucrarea acestor date.

Prelucrarea datelor cu caracter personal se face în conformitate cu prevederile Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor GDPR) precum și cu celelalte legi naționale relevante aplicabile relațiilor de muncă și protecției datelor cu caracter personal.

SPMS JEBEL București va transmite informații despre datele cu caracter personal către terțe părți, în măsura în care va avea obligativitatea de a se alinia prevederilor legale sau de a se conforma clauzelor contractului de muncă semnat de dumneavoastră.

OPERATORUL:

SPMS JEBEL, cu sediul în Jebel, Jud. Timiș, Cod postal 307235, România, este operator de date cu caracter personal și prin urmare este responsabil pentru protecția datelor descrisă mai jos.

Pentru întrebări sau solicitări privind datele cu caracter personal vă rugăm să contactați ofițerul nostru pentru protecția datelor cu caracter personal la datele indicate în prezenta.

RESPONSABILUL DE DATE CU CARACTER PERSONAL:

Puteți contacta ofițerul nostru pentru protecția datelor cu caracter personal la adresa de email: dpo@spitaljebel.ro.

PRELUCRAREA DATELOR CU CARACTER PERSONAL

SPMS JEBEL prelucrează datele dumneavoastră personale în conformitate cu prevederile Regulamentului general privind protecția datelor, ale legilor naționale și europene privind protecția datelor precum și, în calitate de angajator, în conformitate cu prevederile specifice legislației muncii.

SPMS JEBEL va solicita date cu caracter personal în vederea recrutării personalului, pentru stabilirea aptitudinilor necesare și pentru evaluarea experienței profesionale a acestora pentru postul/poziția pentru care se recrutează. În acest sens Serviciul Resurse Umane Normare Organizare și Salarizare, solicită un set de documente pe baza cărora se realizează prelucrarea datelor cu caracter personal. Datele pot include, dar nu se limitează la:

- Date de identificare, contact, statut: nume, prenume, cod numeric personal, data nașterii, telefon mobil personal, adresa de e-mail, starea civilă, etc.;
- Date privind experiența profesională: CV-uri, scrisoare de recomandare, adeverință vechime etc;
- Date legate de studii, competențe: diploma de licență, certificat de specialist sau primar, etc;
- Date privind starea de sănătate: adeverința de la medicul de familie, certificat medical tip A5, etc;
- Date despre infracțiuni sau condamnări definitive, acestea fiind solicitate doar cu respectarea prevederilor legale în vigoare.
- Date financiare.

Prelucrarea datelor cu caracter personal se face având ca temei legal Art. 6 alin. 1 lit. b, și c din Regulamentul general privind protecția datelor (GDPR), respectiv în vederea executării unui contract ce reglementează raportul de muncă (contractul individual de muncă, contractul de management, contractul de voluntariat, etc.), și în vederea îndeplinirii obligațiilor legale ce revin instituției.

NOTĂ DE INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

În conformitate cu prevederile art.12,13 și 14 din Regulamentul general nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestora, **Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel** ca operator date, [mail: secretariat@spitaljebel.ro](mailto:secretariat@spitaljebel.ro), vă informează următoarele:

Prelucrarea datelor dvs. cu caracter personal este necesară **în vederea îndeplinirii actului medical** în conformitate cu următoarele acte normative legale: **Legea 95 / 2006** privind reforma în domeniul sănătății, **Legea 46 / 2003** privind drepturile pacientului, **Legea nr. 190/2018** privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, **H.G. nr. 34 / 2015** privind normele metodologice și modalitatea de utilizare și completare a dosarului electronic de sănătate al pacientului, **Ordinul nr. 1123 / 12.10.2016** privind aprobarea datelor, informațiilor și procedurilor operaționale necesare utilizării și funcționării dosarului electronic de sănătate (DES) al pacientului, **Ordinul nr. 1782 / 2006** privind înregistrarea și raportarea statistică a pacienților care primesc servicii medicale în regim de spitalizare continuă și spitalizare de zi, **Ordinul Ministerului Sănătății nr. 1101/2016** privind aprobarea Normelor de supraveghere, prevenire și limitare a infecțiilor asociate asistenței medicale în unitățile sanitare, **Legea nr. 487/2002** a sănătății mintale și a protecției persoanelor cu tulburări psihice, cu modificările și completările ulterioare.

Datele dvs. personale sunt prelucrate prin sisteme manuale și automate în următoarele scopuri: în cadrul actului medical, [furnizarea de asistență medicală și monitorizarea stării de sănătate, completarea fișelor și formularelor specifice (foaie de observație, formulare medicale, solicitări consult / investigații medicale, informarea medicului trimitor prin scrisoare medicală, bilet de trimitere / întemare, bilet de extemare, concediu medical, efectuarea programărilor, recoltarea probelor biologice și efectuarea buletinelor de analize medicale precum și a testelor solicitate de dvs.); înregistrarea în sistemul informatic (DES); înregistrarea efectuării serviciilor medicale și decontarea acestora, gestionarea programelor naționale de statistică a sănătății, supraveghere video folosind sistemul intern de supraveghere video. Temeiuri legale conform Regulamentului (UE) 2016/679: Art.6(1) c, în vederea îndeplinirii unei obligații legale; Art.6(1) d, pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice; Art.6(1) e, îndeplinirea unei sarcini care servește unui interes public; Art.9(2) h, prelucrarea este necesară în scopuri legate de medicină preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență social, Art.6(1) f, prelucrarea este necesară în scopul intereselor legitime urmărite de operator.

Categoriile de date prelucrate: **datele dvs. personale de identificare:** nume- prenume, CNP, data nașterii, act de identitate (certificat de naștere după caz), adresa de domiciliu, nr. telefon, vârstă, sex, nivel de studii, profesie, ocupație, loc de muncă; **medicale:** statut de asigurat; date despre starea de sănătate actuală, istoricul medical și evoluția bolii (diagnostice, rezultatele investigațiilor medicale și de laborator), tratamentele asociate bolii; **biometrice:** caracteristicile fizice (greutate, înălțime), fiziologice, imagini faciale; **datele personale ale aparținătorilor, sau ale reprezentanților legali** (părinți, tutori, curatori ai pacienților minori și majori fără discernământ, ale rudelor apropiate și/sau ale soțiilor/soților, și/sau ale persoanelor imputabile): nume- prenume, CNP, act de identitate, adresa de domiciliu, calitatea aparținătorului, nr. telefon, numele și prenumele pacientului asistat.

Datele colectate și înregistrate sunt destinate utilizării de către operator, fiind **protejate și transmise** în baza actelor normative către: Ministerul Sănătății, Casa Națională de Asigurări de Sănătate prin Sistemul Informatic Unic Înregistrat (SIUI) pentru raportarea serviciilor medicale în vederea decontării acestora, Casa Județeană de Asigurări de Sănătate, Direcția de Sănătate Publică București, Institutul Național de Sănătate Publică (raportarea cazurilor de boli transmisibile), Direcția Generală de Asistență Socială și Protecția Copilului, etc.

Fără acordul pacientului - datele prelucrate de operator mai pot fi transmise în cazuri și numai în anumite situații speciale, către instanțele judecătorești, organele de cercetare (Parchet, INML), precum și altor instituții la solicitarea scrisă a acestora adresată operatorului, respectiv Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel, specificându-se motivul solicitării și al categoriilor de date necesare, iar către Mass- Media **numai cu acordul pacientului**.

Prelucrarea exactității datelor privind starea de sănătate a pacientului, este efectuată numai de către medic, ori a unui cadru medical sub supravegherea medicului curant, pe durata necesară realizării și îndeplinirii obligațiilor actului medical, cu condiția respectării secretului și al confidențialității profesionale, prin **asigurarea securității adecvate și a protecției împotriva prelucrării neautorizate sau ilegale, a pierderii, distrugerii sau a deteriorării accidentale** a acestor date. Prin măsurile de securitate implementate, se asigură protecția datelor dvs. prelucrate, având o preocupare constantă pentru depistarea, investigarea și soluționarea oricărui tip de atac sau amenințare la adresa securității acestora.

Datele cu caracter personal sunt **stocate și arhivate** pe o perioadă necesară conform normelor medicale, fiscale, contabile sau altor cerințe legislative aplicabile.

Spitalul de Psihiatrie și pentru Măsuri de Siguranță Jebel, ca operator de date, nu va prelucra datele dvs. cu caracter personal care să dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, viața și/sau orientarea sexuală.

Drepturile dvs. cu privire la prelucrarea datelor dvs. personale sunt definite de legislația în vigoare (art.15 la art.23 din Reg. 679 / 2016) în care se menționează: dreptul la informare; dreptul de acces la date și de a solicita o copie a celor colectate și prelucrate; dreptul la rectificarea datelor inexacte și actualizarea lor; dreptul de a solicita ștergerea datelor după expirarea perioadei de păstrare a acestora în măsura în care sunt îndeplinite condițiile prevăzute de lege; dreptul la restricționarea prelucrării; dreptul la portabilitate; dreptul de a vă opune colectării și/sau prelucrării datelor personale, din motive legate de situația particulară existentă.

Dacă protecția datelor dvs. a fost încălcată, aveți dreptul de a vă adresa cu plângere Autorității Naționale de Supraveghere privind Prelucrarea Datelor cu Caracter Personal sau instanțelor competente. Adresa ANSPDCP este B-dul G-ral Gheorghe Magheru nr. 28-30, Sector 1, Buc., telefoane: 0318 059 211, 0318 059 212, email: [anspdcp\[at\]dataprotection.ro](mailto:anspdcp[at]dataprotection.ro), [dpo\[at\]dataprotection.ro](mailto:dpo[at]dataprotection.ro). Pentru exercitarea drepturilor dvs., vă puteți adresa responsabilului cu protecția datelor la adresa de email: dpo@dafcons.ro. Prin semnătură dvs., confirmați că ați luat la cunoștință această notă de informare cu privire la prelucrarea datelor dvs. personale.

Semnătura pacientului: