

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN
DEZNA
JUDEȚUL ARAD

No. 117 / 08.02.2022

Aprobat,
Manager Spital



**PROCEDURA OPERATIONALA
PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU
CARACTER PERSONAL**

COD: P0 - GDPR - 04
Editia 1
Revizia 0

Avizat: presedintele comisiei CIM DR. HANC DANIELA /semnatura/ Daniela
Verificat: responsabil compartiment DUMEA ARIAN /semnatura/ Arian
Elaborat: DUMEA ARIAN
Data aprobarii: 08.02.2022

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I
		Nr. de exemplare: 1
		Revizia: 0
		Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 2 din 12
		Exemplar nr. 1

1. Cuprins:

Numărul componentei în cadrul procedurii operaționale	Denumirea componentei în cadrul procedurii operaționale	Pagina
1.	Cuprins	2
2.	Scopul procedurii operaționale	2
3.	Domeniul de aplicare a procedurii operaționale	2
4.	Documente de referință (reglementări) aplicabile activității procedurate	3
5.	Definiții și abrevieri ale termenilor utilizați în procedura operațională	4
6.	Descrierea procedurii operaționale	5
7.	Responsabilități și răspunderi în derularea activității	10
8.	Formular evidenta modificari	11
9.	Formular analiza procedura	11
10.	Formular distribuire procedura	12
11.	Anexe	12
12.	Diagrama de proces	12

2. Scopul procedurii operaționale:

Prezenta procedura are ca scop stabilirea regulilor și practicilor care reglementează modul în care instituția asigură conformarea cu principiile și regulile stabilite de Regulamentul general privind protecția datelor în activitățile sale de prelucrare a datelor cu caracter personal ale clienților și în relațiile cu furnizori, parteneri, angajați și cu alte părți interesate.

3. Domeniul de aplicare a procedurii operaționale:

3.1. Precizarea (definirea) activității la care se referă procedura operațională:

Procedura este aplicată de către Responsabilul cu protecția datelor și structurile din cadrul Spitalului de Recuperare Neuromotorie „Dr. Corneliu Barsan” Dezna.

3.2. Delimitarea explicită a activității procedurate în cadrul portofoliului de activități desfășurate:

Prezenta procedura gestionează modalitatea de evaluare a impactului asupra protecției datelor cu caracter personal;

3.3. Listarea compartimentelor furnizoare de date și/sau beneficiare de rezultate ale activității procedurate; listarea compartimentelor implicate în procesul activității:

- Compartiment Resurse Umane;
- Compartiment Juridic;
- Compartiment Statistica și Informatica medicală;
- Compartiment de Prevenire a Infecțiilor Asociate Asistentei Medicale (CPIAAM);

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I Nr. de exemplare: 1
		Revizia: 0 Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 3 din 12
		Exemplar nr. 1

- Biroul Managementul Calitatii;
- Bloc Alimentar;
- Compartiment Administrativ;
- Birou Financiar Contabil;
- Compartiment Achizitii Publice Contractare;
- Ambulatoriu integrat:
 - Cabinet Neurologie;
 - Cabinet Recuperare Medicală fizică și Balneologie;
- Secția spitalizare continuă:
 - Secția Recuperare Neuromotorie;
 - Compartiment Recuperare Neuropsihomotorie copii;
 - Compartiment Terapie ocupațională și Ergoterapie;
 - Compartiment Psihologie și Logopedie;
 - Laborator Recuperare Medicală și Balneologie (baza de tratament);
 - Alte structuri – Spălătoria.

4. Documente de referință (reglementări) aplicabile activității procedurate:

4.1. Reglementări internaționale:

- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE - Regulamentul general privind protecția datelor;
- SR ISO 27001:2018 - Tehnologia Informației; Tehnici de securitate. Cerințe pentru un sistem de management al securității informației.

4.2. Legislație primară:

- 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. 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).

4.3. Legislație secundară:

- Ordinul nr. 600 din 20 aprilie 2018 privind aprobarea Codului controlului intern managerial al entităților publice.

4.4. Alte documente, inclusiv reglementări interne ale entității publice:

- Regulamentul de Organizare și Funcționare;
- Regulamentul Intern;
- Fișa postului;

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I Nr. de exemplare: 1
		Revizia: 0 Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 4 din 12
		Exemplar nr. 1

- Alte regulamente, diagrame de proces, etc.

5. Definiții și abrevieri ale termenilor utilizați în procedura operațională:

5.1. Definiții ale termenilor

Procedură documentată - modul specific de realizare a unei activități sau a unui proces, editat pe suport hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem și proceduri operaționale.

Procedura de sistem (procedură generală) - descrie un proces sau o activitate care se desfășoară la nivelul entității publice aplicabil/aplicabilă majorității sau tuturor compartimentelor

Proces - un flux de activități sau o succesiune de activități logic structurate, organizate în scopul atingerii unor obiective definite, care utilizează resurse, adăugându-le valoare.

Ediție procedură - forma actuală a procedurii; editia unei proceduri se modifica atunci cand deja au fost realizate 3 revizii ale respectivei proceduri sau atunci cand modificarile din structura procedurii depasesc 50% din continutul reviziei anterioare

Revizie procedură - actiunea de modificare, respectiv adaugare sau eliminare a unor informatii, date, componente ale unei editii a unei proceduri, modificari ce implica, de regula, sub 50% din continutul procedurii

Gestionarea documentelor - procesul de administrare a documentelor unei entitati publice, pentru a servi intereselor acesteia, pe parcursul intregii lor durate de viata, de la inceput, prin procesul de creare, revizuire, organizare, stocare, utilizare, partajare, identificare, arhivare si pana la distrugerea lor.

Suport informatic - termen general care desemnează mijloacele de înregistrare magnetice, optice sau alte modalități de înregistrare a informațiilor și a căror caracteristică esențială este capacitatea mare de stocare, ștergere, copiere și modificare rapidă și facilă a informațiilor – stik-uri de memorie, CD, HD

Document electronic - document a cărui gestionare se face pe suport informatic.

Fișier electronic - unitate logică și fizică de gestionare a datelor pe suport informatic, care grupează datele pe baza unor caracteristici logice comune.

Sistem de gestiune a fișierelor - aplicații informatice/părți componente ale sistemelor de operare ce oferă suport utilizatorilor în operațiile curente efectuate cu fișiere: creare, actualizare, consultare, ștergere, arhivare.

Destinații (destinatari) de difuzare - locații sau persoane (compartimente/birouri/servicii, funcții) care au acces la un document fie pentru gestionare, fie numai pentru consultare (citire).

Operator – potrivit art. 4 din Regulamentul general privind protecția datelor, înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

Operatori asociați - potrivit art. 26 din Regulamentul (UE) 2016/679, în cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul Regulamentului, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolele 13 și 14, prin intermediul

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I
		Nr. de exemplare: 1
	Cod: PO - GDPR - 04	Revizia: 0
		Nr. de exemplare:
		Pagina 5 din 12
		Exemplar nr. 1

unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

Persoana împuternicită de operator - potrivit art. 4 din Regulamentul (UE) 2016/679, înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

Persoană vizată - orice persoană ale cărei date sunt colectate, reținute sau procesate.

Evaluarea impactului asupra prelucrării DCP - DPIA - reprezintă o modalitate utilă pentru operatorii de date de a implementa sisteme de prelucrare a datelor care respectă GDPR și pot fi obligatorii pentru anumite tipuri de operațiuni de prelucrare. Acestea sunt scalabile și pot lua forme diferite, dar GDPR stabilește cerințele de bază ale unei DPIA eficiente. Operatorii de date ar trebui să considere că realizarea unei DPIA reprezintă o activitate utilă și pozitivă care ajută la respectarea legislației.

5.2. Abrevieri ale termenilor

Nr. Crt.	Abrevierea	Termenul abreviat
1.	PO	Procedura operațională
2.	IL	Instructiune de lucru
3.	E	Elaborare
4.	RI	Regulament Intern
5.	FP	Fisa de post
6.	DCP	Date cu caracter personal
7.	ANSPDCP	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
8.	GDPR	General Data Protection Regulation - Regulamentul general privind protecția datelor

6. Descrierea procedurii operaționale:

6.1. Generalitati

Art. 35 din GDPR introduce conceptual noțiunea de Evaluare a impactului asupra protecției datelor (DPIA2), așa cum prevede și Directiva 2016/680.

DPIA este un process destinat să descrie prelucrarea, să evalueze necesitatea și proporționalitatea acesteia și să contribuie la gestionarea riscurilor la adresa drepturilor și libertăților persoanelor vizate rezultate din prelucrarea datelor cu caracter personal, prin evaluarea acestora și stabilirea de măsuri pentru atenuarea lor.

DPIA reprezintă un instrument important pentru responsabilizare, deoarece ajută operatorii de date nu numai să respecte cerințele GDPR, ci și să demonstreze că au fost luate măsuri adecvate pentru a asigura conformitatea cu Regulamentul (a se vedea de asemenea și art. 24). Cu alte cuvinte, **DPIA reprezintă un proces pentru construirea și demonstrarea conformității.**

Prezenta procedura este proprietatea Spitalului de Recuperare Neuromotorie „Dr. Corneliu Bârsan” Dezna, document controlat, reproducerea neautorizată fiind interzisă.

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I Nr. de exemplare: 1
		Revizia: 0 Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 6 din 12
		Exemplar nr. 1

6.2. Obligația operatorilor de a realiza DPIA

În conformitate cu abordarea bazată pe risc, implementată de GDPR, realizarea unei DPIA nu este obligatorie pentru fiecare operațiune de prelucrare. DPIA este necesară numai atunci când prelucrarea este „susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice” (art. 35 (1)).

Regulamentul general cere operatorilor să implementeze măsuri adecvate pentru a asigura și demonstra conformitatea cu GDPR, luând în considerare, printre altele, „riscurile de variație a probabilității și gravității asupra drepturilor și libertăților persoanelor fizice” (art. 24(1)). Obligația operatorilor de a realiza DPIA în anumite situații ar trebui înțeleasă în contextul obligației lor generale de a gestiona în mod corespunzător riscurile prezentate de prelucrarea datelor cu caracter personal.

Un „risc” reprezintă un scenariu care descrie un eveniment și consecințele acestuia, estimat în termeni de severitate și probabilitate. Pe de altă parte, „managementul riscului” poate fi definit ca fiind activitățile coordonate pentru a conduce și controla o organizație cu privire la un risc.

În situațiile în care nu este clar dacă DPIA este obligatorie, Grupul de lucru Articolul 29 recomandă, totuși, efectuarea unei DPIA ca un instrument util pentru a ajuta operatorii de date să respecte legea privind protecția datelor.

Chiar dacă DPIA ar putea fi solicitată în alte circumstanțe, art. 35 (3) oferă câteva exemple atunci când o operațiune de prelucrare este „susceptibilă să genereze riscuri ridicate”:

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

(b) *prelucrarea pe scară largă a unor categorii speciale de date, menționată la art. 9 (1) sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționat la art. 10; sau*

(c) *monitorizare sistematică pe cară largă a unei zone accesibile publicului”.*

În cazul în care este planificată o prelucrare cu risc ridicat, operatorul de date trebuie:

- să aleagă o metodologie DPIA (exemple prezentate în Anexa 1) care să îndeplinească criteriile din Anexa 2 sau să specifice și să implementeze un proces sistematic și de DPIA care:
 - să fie în conformitate cu criteriile din Anexa 2;
 - este integrat în procesele existente de proiectare, dezvoltare, schimbare, risc și revizuire operațională, în conformitate cu procedurile interne, contextul și cultura;
 - implică părțile interesate și definește în mod clar responsabilitățile acestora (operatorul, DPO, persoanele vizate sau reprezentanții acestora, întreprinderi, servicii tehnice, persoanele împuternicite de operatori, ofițerii de securitate a informațiilor etc.);
- să furnizeze raportul DPIA autorității de supraveghere competente atunci când este necesar să o facă;
- să consulte autoritatea de supraveghere atunci când nu a reușit să stabilească suficiente măsuri pentru atenuarea riscurilor ridicate;
- să revizuiască periodic DPIA și procesele pe care le evaluează, cel puțin atunci când există o schimbare a riscului reprezentat de prelucrarea operațiunii;
- să documenteze deciziile luate.

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I Nr. de exemplare: 1
		Revizia: 0 Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 7 din 12
		Exemplar nr. 1

6.3. Criteriile evaluării de impact

Pentru a oferi un set mai precis de operațiuni de prelucrare care necesită o DPIA datorită riscului ridicat inerent, trebuie luate în considerare următoarele **nouă criterii**.

1. Evaluarea sau scoring, inclusiv profilarea și preconizarea, în special din „aspecte privind performanța persoanei vizate la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările” (Considerentele 71 și 91).

2. Proces decizional automatizat cu efecte legale sau similare semnificative: prelucrare care vizează luarea deciziilor asupra persoanelor vizate care produc „efecte juridice privind persoana fizică” sau care „o afectează în mod similar într-o măsură semnificativă” (art. 35 (3) a)). Spre exemplu, prelucrarea poate conduce la excluderea sau discriminarea persoanelor. Prelucrarea cu efect redus sau fără efect asupra persoanelor nu corespunde acestui criteriu specific.

3. Monitorizare sistematică: prelucrare folosită pentru a observa, monitoriza sau controla persoanele vizate, incluzând colectarea de date prin rețele sau „monitorizarea sistematică a unei zone accesibile publicului” (art. 35 (3) c)). Acest tip de monitorizare reprezintă un criteriu deoarece datele cu caracter personal pot fi colectate în situații în care persoanele vizate pot să nu fie conștiente de cine colectează datele și modul în care acestea vor fi utilizate. În plus, poate fi imposibil ca persoanele să nu fie supuse unei astfel de prelucrări în spațiul (sau zonele publice) accesibile publicului.

4. Date sensibile sau date de natură foarte personală: acestea includ categorii speciale de date cu caracter personal așa cum sunt definite în art. 9 (spre exemplu, informații privind opiniile politice ale persoanelor fizice), precum și date cu caracter personal privind condamnările penale sau infracțiuni așa cum sunt definite în art. 10.

Dincolo de aceste prevederi ale GDPR, anumite categorii de date pot fi considerate că ar crește riscul posibil pentru drepturile și libertățile persoanelor. Aceste date cu caracter personal sunt considerate ca fiind date sensibile (deoarece acest termen este înțeles în mod obișnuit) deoarece sunt legate de activitățile casnice și private (cum ar fi comunicațiile electronice a căror confidențialitate ar trebui protejată) sau deoarece respectivele date influențează exercitarea unui drept fundamental (cum ar fi datele de localizare a căror colectare pune la îndoială libertatea de mișcare) sau pentru că încălcarea lor implică în mod clar efecte grave asupra vieții de zi cu zi a persoanei vizate (cum ar fi datele financiare care ar putea fi folosite pentru fraudarea plăților). În acest sens, ar putea fi relevant dacă datele au fost deja puse la dispoziția publicului de către persoana vizată sau de terți. Faptul că datele cu caracter personal sunt disponibile în mod public poate fi considerat un factor în evaluarea dacă datele se preconizează a fi utilizate în continuare în anumite scopuri. Acest criteriu poate include, de asemenea, date cum ar fi documentele personale, e-mailurile, jurnalele, notele de la cititorii electronici echipate cu funcții de notare și informații foarte personale conținute în aplicațiile de log.

5. Date prelucrate pe scară largă: GDPR nu definește ce înseamnă scară largă, însă Considerentul 91 oferă anumite linii directoare. În orice caz, Grupul de lucru Articolul 29 recomandă luarea în considerare, în special, a următorilor factori pentru a se determina dacă o prelucrare este efectuată pe scară largă:

- a. numărul persoanelor vizate, ori un număr exact ori un procent din populația relevantă;
- b. volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
- c. durata sau permanența activității de prelucrare a datelor;
- d. suprafața geografică a activității de prelucrare.

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I Nr. de exemplare: 1
		Revizia: 0 Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 8 din 12
		Exemplar nr. 1

6. Potrivirea sau combinarea seturilor de date, spre exemplu, provenind de la două sau mai multe operațiuni de prelucrare a datelor efectuate în scopuri diferite și/sau de diverși operatori de date într-un mod care ar depăși așteptările rezonabile ale persoanei vizate.

7. Date privind persoanele vizate vulnerabile (Considerentul 75): prelucrarea acestui tip de date este un criteriu din cauza dezechilibrului de putere crescut între persoanele vizate și operatorul de date, ceea ce înseamnă că persoanele ar putea să nu fie în stare să își dea cu ușurință consimțământul sau să se opună prelucrării datelor lor sau să își exercite drepturile. Persoanele vizate vulnerabile pot include copiii (pot fi considerați incapabili să se opună sau să consimtă sau să se opună în mod deliberat la prelucrarea datelor lor), angajați, segmente mai vulnerabile ale populației care necesită protecție specială (persoane bolnave, solicitanți de azil sau vârstnici, pacienți etc.) și, în orice caz, poate fi identificat un dezechilibru în relația dintre poziția persoanei vizate și operator.

8. Utilizare inovatoare sau implementarea unor noi soluții tehnologice sau organizaționale, cum ar fi combinarea utilizării amprentei digitale cu recunoașterea facială pentru îmbunătățirea controlului accesului fizic etc. GDPR clarifică (art. 35 (1) și Considerentele 89 și 91) faptul că utilizarea unei noi tehnologii, definită în „conformitate cu nivelul atins al cunoștințelor tehnologice” (Considerentul 91), poate declanșa necesitatea realizării unei DPIA. Acest lucru se datorează faptului că utilizarea unei astfel de tehnologii poate implica noi forme de colectare și utilizare a datelor, eventual cu un risc ridicat pentru drepturile și libertățile persoanelor fizice. Într-adevăr, consecințele personale și sociale ale desfășurării unei noi tehnologii pot fi necunoscute. O DPIA va ajuta operatorul să înțeleagă și să abordeze astfel de riscuri. Spre exemplu, anumite aplicații „Internet of Things” ar putea avea un impact semnificativ asupra vieții cotidiene și a vieții private a persoanelor fizice; și, prin urmare, necesită o DPIA.

9. Atunci când prelucrarea în sine „împiedică persoanele fizice să-și exercite un drept sau să utilizeze un serviciu sau un contract” (art. 22 și Considerentul 91). Acestea includ operațiuni de prelucrare care vizează permiterea, modificarea sau refuzarea accesului persoanelor fizice la un serviciu.

Ca parte a principiului responsabilității, fiecare operator de date „va păstra o evidență a activităților de prelucrare desfășurate sub responsabilitatea sa” ce va cuprinde, printre altele, scopurile prelucrării, o descriere a categoriilor de date și destinatarii datelor și „acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la art. 32 (1)” (art. 30 (1)) și trebuie să evalueze dacă există un risc ridicat, chiar dacă decid în cele din urmă să nu realizeze o DPIA.

6.4 Când nu este necesară DPIA

Grupul de lucru Articolul 29 consideră că DPIA nu este necesară în următoarele situații:

- atunci când prelucrarea nu este „susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice” (art. 35 (1));
- atunci când natura, obiectivul, contextul și scopurile prelucrării sunt similare prelucrării pentru care a fost realizată DPIA. În astfel de situații, pot fi utilizate rezultatele DPIA pentru prelucrări similare (art. 35 (1));
- atunci când operațiunile de prelucrare au fost verificate de autoritatea de supraveghere înainte de mai 2018 în condiții specifice care nu au suferit modificări (a se vedea III.C);
- atunci când operațiunea de prelucrare, potrivit literelor c) și e) de la art. 6 (1), are un temei juridic în dreptul Uniunii sau al unui stat membru, iar dreptul respectiv reglementează operațiunea de prelucrare și deja s-a efectuat o DPIA ca parte a unei evaluări a impactului general în contextul adoptării

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I Nr. de exemplare: 1
		Revizia: 0 Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 9 din 12
		Exemplar nr. 1

respectivului temei juridic (art. 35 (10)), cu excepția cazului în care statul membru a declarat că este necesară efectuarea unei astfel de DPIA înaintea desfășurării activităților de prelucrare;

- atunci când prelucrarea este inclusă pe lista opțională (stabilită de autoritatea de supraveghere) a operațiunilor de prelucrare pentru care nu este necesară DPIA (art. 35 (5)).

O astfel de listă poate conține activități de prelucrare care respectă condițiile specificate de această autoritate, în special prin ghiduri, decizii sau autorizații specifice, reguli de conformitate etc. În astfel de cazuri și sub rezerva reevaluării de către autoritatea de supraveghere competentă, o DPIA nu este necesară, ci numai dacă prelucrarea intră strict în sfera procedurii relevante menționate în listă și continuă să respecte pe deplin toate cerințele relevante din GDPR.

6.5 Efectuarea unei DPIA este un proces continuu, nu un exercițiu unic.

Cine are obligația să efectueze DPIA? Operatorul, împreună cu DPO și împuterniciții.

Operatorul este responsabil pentru realizarea unei DPIA (art. 35 (2)). DPIA poate fi realizată și de altcineva din interiorul sau exteriorul organizației, dar operatorul rămâne în cele din urmă responsabil pentru această sarcină.

De asemenea, **operatorul trebuie să solicite avizul Responsabilului cu protecția datelor (DPO)**, în cazul în care acesta este desemnat (art. 35 (2)) și acest aviz, precum și deciziile luate de operator, ar trebui să fie documentate în cadrul DPIA. De asemenea, DPO ar trebui să monitorizeze funcționarea DPIA (art. 39 (1) litera (c)). Ghidul Grupului de lucru Articolul 29 privind responsabilul cu protecția datelor 16/EN WP 243 oferă instrucțiuni suplimentare.

Dacă prelucrarea este efectuată parțial sau în totalitate de persoana împuternicită de operator, **persoana împuternicită de operator va ajuta operatorul la realizarea DPIA** și va oferi informațiile necesare (în conformitate cu art. 28 (3) litera f)).

6.6 Metodologia pentru efectuarea DPIA

GDPR stabilește caracteristicile minime ale unei DPIA (art. 35 (7) și Considerentele 84 și 90):

- o descriere a operațiunilor de prelucrare preconizate și scopurilor prelucrării;
- o evaluare a necesității și proporționalității prelucrării;
- o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate;
- măsurile preconizate în vederea:

- abordării riscurilor
- demonstrării conformității cu dispozițiile prezentului Regulament.

Trebuie avută în vedere respectarea (art 35 (8)) unui cod de conduită (art. 40) atunci când se evaluează impactul unei operațiuni de prelucrare a datelor. Acest lucru poate fi util pentru a demonstra că au fost alese sau introduse măsuri adecvate, cu condiția ca respectivul cod de conduită să fie adecvat operațiunii de prelucrare.

6.7 Consultarea ANSPDCP

Este necesară consultarea cu autoritatea de supraveghere de fiecare dată când operatorul de date nu poate găsi suficiente măsuri pentru a reduce riscurile la un nivel acceptabil (adică riscurile reziduale sunt încă ridicate).

În plus, operatorul va trebui să consulte autoritatea de supraveghere și/sau să obțină autorizarea prealabilă din partea acesteia în ceea ce privește prelucrarea de către un operator pentru îndeplinirea unei sarcini

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I
		Nr. de exemplare: 1
		Revizia: 0
		Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 10 din 12
		Exemplar nr. 1

exercitate de operator în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică (art. 36 (5)).

Cu toate acestea, trebuie precizat faptul că obligațiile de a păstra o evidență a DPIA și de a actualiza DPIA în timp util rămân, indiferent dacă este necesară sau nu consultarea autorității de supraveghere în funcție de nivelul riscului rezidual.

6.8 Sancțiuni

Potrivit GDPR, nerespectarea cerințelor DPIA poate conduce la aplicarea de amenzi de către autoritatea de supraveghere. Nerealizarea unei DPIA atunci când prelucrarea face obiectul unei DPIA (art. 35 (1) și (3) - (4)), realizarea unei DPIA într-un mod incorect (art. 35 (2) și (7) – (9)) sau dacă nu se consultă cu autoritatea de supraveghere competentă, dacă este cazul (art. 36 (3) litera (e)), poate conduce la o amendă administrativă de până la 10 milioane EUR sau, în cazul unei întreprinderi, până la 2% din cifra de afaceri globală anuală, oricare dintre acestea este mai mare.

6.9. Documente utilizate

Lista și proveniența documentelor

- Nomenclatorul arhivistic.

Conținutul și rolul documentelor

- Conținutul documentelor este prezentat la prezenta procedura.

Circuitul documentelor

- Grafic de circulație a documentelor aprobat la nivel de instituție.

6.10. Resursele necesare

Resurse materiale

- conform Necesarului de materiale - stabilit.

Resurse umane

- conform organigramei entității.

Resurse financiare

- planificarea activităților se realizează pe baza Bugetului de venituri și cheltuieli.
- determinarea fondurilor necesare se face anual - în trimestrul IV al anului în curs pentru anul următor.

7. Responsabilități și răspunderi în derularea activității:

7.1. Manager spital

- Aproba/reaproba prezenta procedura;
- Conform descrierii din procedură.

7.2. Responsabilii de compartimente/servicii/birouri din cadrul instituției:

- Conform descrierii din procedură.

7.4. Responsabilul de protecția DCP

- să furnizeze consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și să monitorizeze funcționarea acesteia, în conformitate cu art. 35 din Regulamentul (UE) 679/2016;

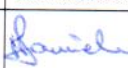
SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I Nr. de exemplare: 1
		Revizia: 0 Nr. de exemplare:
	Cod: PO - GDPR - 04	Pagina 11 din 12
		Exemplar nr. 1

- să acorde avizul solicitat de conducerea instituției în legătură cu următoarele aspecte:
1. dacă să efectueze sau nu evaluarea impactului asupra protecției datelor;
 2. ce metodologie să fie folosită la efectuarea evaluării impactului asupra protecției datelor;
 3. dacă să efectueze intern sau să externalizeze evaluarea impactului asupra protecției datelor;
 4. ce garanții (inclusiv măsuri tehnice și organizaționale) să pună în aplicare pentru reducerea oricăror riscuri la adresa drepturilor și intereselor persoanelor vizate;
 5. dacă evaluarea impactului asupra protecției datelor a fost sau nu efectuată corect și dacă respectivele concluzii (dacă să continue sau nu prelucrarea și ce garanții să pună în aplicare) respectă Regulamentul (UE) 2016/679;
 6. să prioritizeze activitățile sale și să-și concentreze eforturile asupra problemelor care prezintă riscuri mai mari pentru protecția datelor.
 7. să participe la ședințele Comisiei de monitorizare.

8. Formular evidență modificări:





Nr. Crt.	Editie	Data editiei	Revizie	Data reviziei	Nr. pagina modificata	Descriere modificare	Semnatura responsabil compartiment
1	2	3	4	5	6	7	8
	1		0			Procedura a fost elaborata in conf. Cu Ord. 600/2018	

9. Formular analiză procedură:

Nr. crt	Compartiment	Nume si prenume responsabil compartiment	Inlocuitor de drept sau delegat	Aviz favorabil		Aviz nefavorabil		
				Data	Semnatura	Observatii	Data	Semnatura
1.	SCIM	DR. HANU DANIELA		08.02				
2.								
3.								

SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN DEZNA	PROCEDURA OPERATIONALA PRIVIND EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL	Ediția: I Nr. de exemplare: 1
	Cod: PO - GDPR - 04	Revizia: 0 Nr. de exemplare: Pagina 12 din 12 Exemplar nr. 1

10. Formular distribuire procedură:

Nr. Crt.	Scopul difuzării	Compartiment	Funcția	Nume și prenume	Data primirii	Data retragerii	Semnătură
10.1.	informare	Secretariat SCIM		CRISTEA L.	08.02.2022		
10.2.	aplicare	Serviciu extern de contact		NINEA A.	08.02.2022		
10.3.	evidenta	Secretariat SCIM		CRISTEA L.	08.02.2022		
10.4.	arhivare	Secretariat SCIM		CRISTEA L.	08.02.2022		

11. Anexe:

- Conform legislației în vigoare.

12. Diagrama de proces