

CC Guvernare, Conducere, Orientare

PROCEDURĂ OPERAȚIONALĂ STANDART

PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

POS: GCO - 03

SCOPUL PREZENTEI PROCEDURI este asigurarea protecției drepturilor și libertăților fundamentale ale persoanelor în ce privește prelucrarea datelor cu caracter personal, responsabilitățile concrete ale subiecților implicați în procesul de prelucrare și stocare a lor, de a identifica eventualele riscuri și a stabili măsuri de reducere a lor.

DOMENIUL DE APLICARE A POS

Prevederile cuprinse în această procedură operațională se adresează tuturor angajaților IMSP „Timofei Moșneaga” care prelucrează sau stochează date cu caracter personal.

Documente de referință

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);
- DIRECTIVA (UE) 2016/680 a parlamentului european și a consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului

Reglementări naționale:

- Constituția Republicii Moldova;
- Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal;
- Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
- Ordinul nr. 27 din 31 martie 2022 privind aprobarea Listei tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor cu caracter personal, emis de Centru național pentru protecția datelor cu caracter personal.

Ce reprezintă datele cu caracter personal?

Orice informație care poate identifica o persoană fizică direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale

Exemple de datele cu caracter personal

- nume și prenume
- adresă de domiciliu
- adresă de e-mail, cum ar fi prenume.nume@societate.com
- număr de act de identitate
- date privind locația (de exemplu, funcția de date privind locația disponibilă pe un telefon mobil)* etc.

Prelucrarea Datelor cu caracter personal?

Fără consimțământul subiectului este necesară:

- protecția vieții, integrității fizice sau a sănătății în cazul în care subiectul se află în incapacitate fizică sau juridică de a-și da consimțământul
- îndeplinirea obligațiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii
- în contextul activităților legitime de către asociații obștești, partide și alte organizații social-politice, religioase, etc. cu condiția ca prelucrarea să se refere numai la membrii acestora
- pentru constatarea, exercitarea sau apărarea unui drept în justiție al subiectului datelor cu caracter personal
- în scopul asigurării securității statului, al reducerii riscului de declanșare sau în cazul declanșării urgențelor de sănătate publică
- efectuarea auditului public extern
- în scopuri statistice, de cercetare istorică sau științifică, cu condiția ca datele cu caracter personal să rămână anonime pe toată durata prelucrării
- la date făcute publice în mod voluntar și manifest de către subiectul datelor cu caracter personal

Consimțământul pacientului privind prelucrarea datelor cu caracter personal

nu este necesar a fi întocmit în formă scrisă având în vedere excepția prevăzută de art. 5 alin. (5) lit.b), c), d) din legea nr. 133 din 08.07.2011, potrivit căruia pot fi prelucrate date privind starea de sănătate atunci când prelucrarea este necesară din motive de interes public major sau pe motivul protejării vieții, sănătății subiectului datelor cu caracter personal sau îndeplinirii unei obligații care îi revine operatorului/institutiei medicale conform legii

Informația privind starea de sănătate, rezultatele investigațiilor, diagnosticul, pronosticul, tratamentul, datele privind consumul de medicamente, alcool, droguri, datele administrative cum ar fi numărul poliței de asigurare medicală, faptul internării în spital, precum și datele genetice reprezintă date cu caracter medical privind starea de sănătate, sunt confidențiale și urmează a fi protejate de către personalul medico-sanitar

Toate cadrele medicale/auxiliare care au acces la date cu caracter personal urmează a fi supuse unei clauze de confidențialitate, care va fi inclusă în contractele de muncă sau/și în fișa postului cu mențiunea despre posibilitatea atragerii la răspundere civilă, contravențională ori penală pentru încălcarea acesteia;

Consimțământul angajaților privind prelucrarea datelor cu caracter personal

Angajatorul și reprezentanții lui sunt obligați să respecte următoarele cerințe:

- a) Prelucrarea poate fi efectuată exclusiv în scopul:
 - acordării de asistență la angajare,
 - instruirii și avansării în serviciu,
 - asigurării securității personale a salariatului,
 - controlului volumului și calității lucrului îndeplinit și asigurării integrității bunurilor unității;
- b) toate datele personale urmează a fi preluate de la salariat sau din sursa indicată de acesta.
- c) nu este în drept să obțină și să prelucreze date referitoare la convingerile politice și religioase ale salariatului, precum și la viața privată a acestuia fără acordul scris al acestuia.
- d) protecția datelor personale ale salariatului contra utilizării ilegale sau pierderii este asigurată din contul angajatorului.

Măsuri privind protecția datelor cu caracter personal

Angajații instituției medicale care folosesc date cu caracter personal sunt obligați să respecte următoarele măsuri:

parole calitative cu o mărime de minimum 8 simboluri, care nu sunt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sunt compuse integral din grupuri de cifre sau litere

să dezactiveze procesul automatizat de înregistrare (cu folosirea parolelor salvate)

să deconecteze computerele, terminalele de acces și imprimantele la terminarea sesiunilor de lucru

este interzisă instalarea programelor de tip Shareware sau freeware (care pot fi utilizate gratuit doar pe o perioadă scurtă), fără aprobarea administratorului sistemului informatic

să păstreze în safeuri sau dulapuri care se încuie purtători de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal

Măsuri privind protecția datelor cu caracter personal

Se pune în sarcina Serviciului Informațional și Telecomunicații:

Să creeze pentru toți utilizatorii un identificador personal (ID-ul utilizatorului) inclusiv pentru personalul non medical

Să implementeze tehnici pentru a limita accesul la distanță și folosirea tehnologiei fără fir

Să elaboreze reguli și proceduri de securitate a sistemului IT din cadrul instituției

Să verifice periodic calculatoarele pentru a asigura protecție contra programelor dăunătoare (virusilor)

Să creeze pentru toți utilizatorii un identificador personal (ID-ul utilizatorului) inclusiv pentru personalul non medical

Să se asigure că angajații folosesc metodele de cifrare a informației, precum și utilizarea canalelor VPN, etc.

Să revoce sau să suspende codurile să monitorizeze toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal (utilizându-se VPN, criptarea, cifrarea etc.) e identificare și autentificare în cazul în care contractul de muncă /raporturile de serviciu ale utilizatorului au fost încetate, etc.

Măsuri privind protecția datelor cu caracter personal

Se pune în sarcina Serviciului protecție civilă, securitatea muncii și obiectului:

Să asigure securitatea contra accesului neautorizat, furturilor, incendiilor, inundațiilor și altor posibile riscuri. Ușile și ferestrele se fie încuiate în cazul în care în încăpere lipsesc angajații, sediul să fie asigurat cu pază permanentă 24/24

Să se asigure că accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal să fie restricționat, intrările să fie echipate cu lacăte și semnalizare sau control acces

Să asigure controlul instalării și scoaterii componentelor IT din sediul instituției medicale

Să asigure securitatea sediilor și mijloacelor de prelucrare a datelor cu caracter personal

Să monitorizeze accesului fizic și controlul vizitatorilor

Măsuri privind protecția datelor cu caracter personal

Se pune în sarcina Serviciului antiincendiar:

Să implementeze sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sunt amplasate sistemele informaționale și mijloacele de prelucrare de date cu caracter personal

În cazul apariției situațiilor forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI

Să verifice periodic, dar nu mai puțin de o dată în semestru, securitatea electroenergetică a cablurilor de rețea

Să se asigure că echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesanctionate

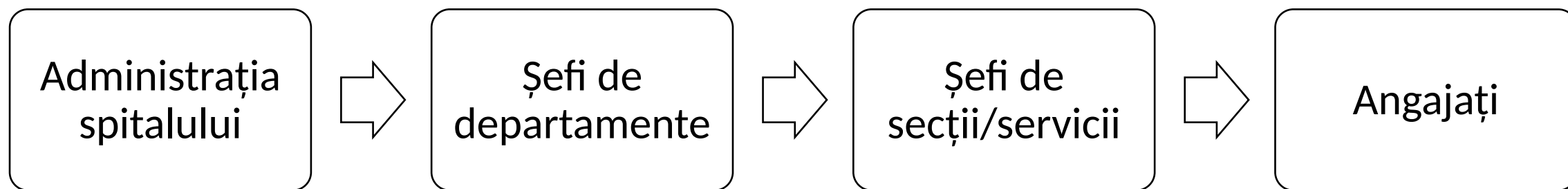
Evaluarea impactului asupra datelor cu caracter personal

- Descriere sistematică a operațiunilor de prelucrare și a scopurilor prelucrării inclusiv, interesul legitim urmărit de operator
- O evaluare a necesității și proporționalității operațiunilor de prelucrare
- O evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate
- Măsuri preconizate în vederea abordării riscurilor, măsuri de securitate, mecanisme menite să asigure protecția datelor cu caracter personal

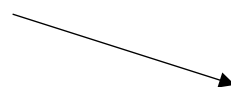
- Evaluarea impactului datelor cu caracter personal va fi făcută de fiecare serviciu/secție sub ghidarea persoanei responsabile de protecția datelor
- Instituția desemnează persoană responsabilă de protecția datelor în spital
- Raportarea incidentelor se va face verbal sau scris de oricine la adresa de email **datepersonale@scr.md**
- Incidentele asupra DCP vor fi colectate de către persoana desemnată responsabilă de protecția datelor în instituție.

Controlul respectării datelor cu caracter personal

- Controlul intern



- Controlul extern:



POS privind elaborarea procedurilor

Nr. Crt.	Ediția/revizia în cadrul ediției	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediției sau reviziei ediției
	1			
2.1.	Ediția 2	X	X	
2.2.	Revizia 1	p.7.3. p.8 p.10	Modificat Anulat Completat	

Revizia
1

POS privind evaluarea satisfacției pacientului

Nr. Crt.	Ediția/revizia în cadrul ediției	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediției sau reviziei ediției
	1			
2.1.	Ediția 2	X	X	
2.2.	Revizia 1	P.7.2.; 7.4. P.8. P.9.	Modificat Modificat Modificat	

Revizia
1

POS privind evaluarea satisfacției personalului

Nr. Crt.	Ediția/revizia în cadrul ediției	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediției sau reviziei ediției
	1			
2.1.	Ediția 2	X	X	
2.2.	Revizia 1	P.7.2.; 7.4. P.8. P.9.	Modificat Modificat Modificat	

Revizia
1