Protectia datelor personale

INSTRUCTIUNI PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

In conformitate cu 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), va facem cunoscute urmatoarele atributii pentru a îndeplini cerinţele minime de securitate a prelucrărilor de date cu caracter personal:

- prelucrarea datelor se va face numai de către utilizatori desemnaţi;
- utilizitorii desemnaţi vor accesa datele cu caracter personal numai in interes de serviciu;
- operatorii care au acces la date cu caracter personal au obligaţia de păstra confidenţialitatea acestora;
- se interzice folosirea de către utilizatori a programelor software care provin din surse externe sau dubioase, existând riscul ca odata cu accesarea acestor programe sa pătrundă in sistem viruşi informatici ce pot distruge bazele de date existente; se interzice descarcarea de pe internet a altor programe decât cele instalate de personalul compartimentului de informatica, a fişierelor cu muzica, filme, poze etc;
- operatorii sunt obligaţi sa isi inchida sesiunea de lucru atunci cand părăsesc locul de munca;
- încăperile unde sunt amplasate calculatoarele trebuie sa fie încuiate atunci cand nu se afla nimeni acolo;
- terminalele de acces folosite vor fi pozitionate astfel incat sa nu poata fi văzute de public;
- utilizatorul care primeşte un cod de identificare si un mijloc de autentificare trebuie sa păstreze confidenţialitatea acestora.
- încalcarea acestor dispoziţii poate duce la interzicerea accesului la sistemul informatic sau chiar la sanctionarea disciplinara a salariatului.

I. Instructiuni privind conditiile si obligatiile pentru prelucrarea electronica a datelor cu caracter personal

Domeniul de aplicare a Regulamentului (UE) 2016/679

Prezentul regulament se aplică:

- prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.
- prelucrării datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.
- prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator care nu este stabilit(ă) în Uniune, atunci când activităţile de prelucrare sunt legate de: oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana

vizată; sau monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

- prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internaţional public.

Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

- în cadrul unei activităţi care nu intră sub incidenţa dreptului Uniunii;
- de către statele membre atunci când desfăşoară activităţi care intră sub incidenţa capitolului 2 al titlului V din Tratatul UE;
- de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice;
- de către autorităţile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracţiunilor, sau al executării sancţiunilor penale, inclusiv al protejării împotriva ameninţărilor la adresa siguranţei publice şi al prevenirii acestora.

Legalitatea prelucrărilor de date cu caracter personal

Prelucrarea este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele condiţii:

a) persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului;

d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul;

f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Litera (f) din nu se aplică în cazul prelucrării efectuate de autorităţi publice în îndeplinirea atribuţiilor lor.

II. Persoanele fizice sau juridice cărora li se aplică dispoziţiile Regulamentului UE 679/2016:

- Operatorul de date cu caracter personal – înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi 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.
- Persoana împuternicită de către operator – înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
- Destinatar - înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul

Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

- Parte terţă - înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

III. Obligaţiile operatorilor de date cu caracter personal

Potrivit prevederilor Regulamantului UE 679/2016, operatorii au următoarele responsabilități:

- Ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu cerințele regulamentului. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.
- Atunci când sunt proporţionale în raport cu operaţiunile de prelucrare, măsurile menţionate anterior includ punerea în aplicare de către operator a unor politici adecvate de protecţie a datelor.
- Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal. Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecţiei datelor indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului.
- Aderarea la coduri de conduită aprobate sau la un mecanism de certificare aprobat, care să demonstreze respectarea obligaţiilor de către operator.
- În cazul în care doi sau mai mulţi operatori stabilesc în comun scopurile şi mijloacele de prelucrare, aceştia sunt operatori asociaţi. Ei stabilesc într-un mod transparent responsabilităţile fiecăruia în ceea ce priveşte îndeplinirea obligaţiilor care le revin în temeiul regulamentului, în special în ceea ce priveşte exercitarea drepturilor persoanelor vizate şi îndatoririle fiecăruia de furnizare a informaţiilor către persoanele vizate, prin intermediul unui acord între ei.
- În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în regulament şi să asigure protecţia drepturilor persoanei vizate.
- Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului.
- Fiecare operator şi, după caz, reprezentantul acestuia păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea lor. Evidenţele se formulează în scris, inclusiv în format electronic. Operatorul şi reprezentantul operatorului pun evidenţele la dispoziţia autorităţii de supraveghere, la cererea acesteia.

- Operatorul şi reprezentantul acestuia cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor lor.
- În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, operatorul notifică acest lucru autorităţii de supraveghere competente, fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice.
- Operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse.
- În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.
- Operatorul desemnează un responsabil cu protecţia datelor dacă prelucrarea este efectuată de o autoritate sau un organism public, dacă activităţile principale ale operatorului constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară largă sau dacă activităţile principale ale operatorului constau în prelucrarea pe scară largă a unor categorii speciale de date.
- Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecţia datelor şi le comunică autorităţii de supraveghere.

IV.Drepturile persoanei vizate în contextul prelucrării datelor cu caracter personal

Persoanele vizate de prelucrări au un număr de drepturi în cadrul Regulamentului UE 679/2016. Acestea includ:

- **Dreptul la transparenţa** informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate.

- **Dreptul de acces**. Persoana vizată are dreptul de a obţine din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc şi, în caz afirmativ, acces la datele respective. Dreptul de a obţine o copie a datelor deţinute nu trebuie să aducă atingere drepturilor şi libertăţilor altor persoane.

-**Dreptul la rectificare**. Reprezintă dreptul persoanei vizate de a solicita operatorului să remedieze inexactităţile privind datele cu caracter personal stocate în legătură cu acesta. În anumite circumstanţe, dacă datele cu caracter personal sunt incomplete, o persoană poate cere operatorului să completeze datele sau să înregistreze informații suplimentare.

-Dreptul de a fi uitat (ștergerea). În anumite situații, persoanele vizate au dreptul să solicite ca datele lor să fie șterse. De exemplu, acest drept se aplică în cazul în care datele nu mai sunt necesare pentru scopul pentru care au fost colectate sau dacă individul își retrage consimțământul sau dacă informația este prelucrată ilegal. Există cateva excepții: dacă prelucrarea se face în scopuri științifice sau istorice, de cercetare sau în scopuri statistice, iar ștergerea datelor ar face imposibilă sau ar afecta grav îndeplinirea obiectivelor.

- **Dreptul la restricţionarea prelucrării**. În anumite cazuri, persoana vizată are dreptul de a obţine din partea operatorului restricţionarea prelucrării pentru o anumită perioadă de timp în

care operatorul trebuie să verifice exactitatea datelor sau să verifice dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

-Dreptul la portabilitate. Persoana vizată are dreptul de a solicita ca informațiile să-i fie furnizate într-o formă structurată, frecvent utilizată, care să poată fi interpretată automat prin intermediul unui program informatic, astfel încât aceasta să poată fi trimisă altui operator de date. Acest lucru se aplică numai datelor cu caracter personal care sunt prelucrate prin mijloace automate (nu pe hârtie), datelor cu caracter personal pe care persoana vizată le-a furnizat operatorului și numai atunci când prelucrarea se face pe baza consimțământului sau a unui contract.

- **Dreptul la opoziție**. Persoanele vizate au dreptul de a formula obiecții față de anumite tipuri de prelucrări. Exceptând cazul în care prelucrarea datelor se face în scopul marketing-ului direct (inclusiv, profilarea în scop de marketing direct), persoana vizată trebuie să demonstreze motivele pentru care se opune unei prelucrări.

-Drepturi legate de luarea deciziilor și profilarea automată. Dreptul se referă la decizii sau profiluri automate care ar putea avea ca rezultat efecte semnificative asupra unui individ. Persoanele vizate au dreptul să nu se supună deciziilor bazate exclusiv pe prelucrarea automată. Atunci când se utilizează profilarea, trebuie luate măsuri pentru a asigura securitatea și fiabilitatea serviciilor. Decizia automată bazată pe date sensibile poate fi făcută numai cu acordul explicit al persoanei vizate.

SUPRAVEGHEREA VIDEO

Utilizarea sistemului de supraveghere video este necesară pentru a menține un climat social optim și pentru a spori siguranța, securitatea și controlul accesului, deasemenea sistemul este folosit pentru prevenirea și combaterea infracționalității fapt menționat și pe pictogramele poziționate la o distanță rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere video, în incinta Spitalului, așa cum este prevăzut de Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, de Regulament UE nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) și de Directivele Autorităţii Europene de Protecţie a Datelor Personale privind supravegherea video.

1. SCOPUL SUPRAVEGHERII VIDEO

Spitalul utilizează sistemul de supraveghere video pentru a garanta siguranța, securitatea și controlul accesului. Sistemul de supraveghere contribuie la controlarea accesului în clădirile noastre și asigură securitatea și siguranța clădirilor, a personalului, pacienților și a vizitatorilor, precum și a bunurilor și documentelor prezente sau păstrate în spital.
Sistemul de supraveghere video ajută la prevenirea, descurajarea, gestionarea și, dacă este necesar, anchetarea incidentelor legate de siguranță și securitate, a potențialelor amenințări sau a accesului fizic neautorizat, inclusiv a accesului neautorizat în clădiri și în diferite camere, la infrastructura IT sau la aparatura de investigație medicala existentă.
Sistemul nu este utilizat în alte scopuri decât cele menționate mai sus. De exemplu, nu este

utilizat pentru a monitoriza prezența angajaților. Sistemul nu este utilizat nici ca instrument de anchetă în alte scopuri decât cele descrise mai sus, cu excepția cazului în care este vorba de un incident de siguranță fizică sau de o infracțiune.
Înregistrările pot fi transmise organelor de anchetă în cadrul unei anchete disciplinare sau penale oficiale in baza unor solicitari scrise a acestora.

2. CATEGORII SPECIALE DE DATE

Sistemul de supraveghere video al Spitalului nu are drept scop colectarea unor categorii speciale de date, cum ar fi originea rasială sau etnică, opiniile politice, credințele religioase sau filosofice, apartenența la sindicate sau date privind sănătatea sau orientarea sexuală.
Sistemul de supraveghere monitorizează aria minimă necesară pentru a asigura siguranța și securitatea clădirilor, accesul si zonele speciale. Având în vedere nivelul înalt al expunerii clădirilor spitalului din perspectiva securității (perimetrul este ușor accesibil), intrările și perimetrul spitalului sunt echipate cu camere de supraveghere. Scopul utilizării acestor camere nu este de a înregistra sau procesa categorii speciale de date, nici de a viza un individ, ci de a fi capabil de a preveni, a evalua și a ancheta incidente legate de securitate.

3. ZONELE AFLATE SUB SUPRAVEGHERE

Amplasarea camerelor de supraveghere și a unghiurilor de vizionare ale acestora se bazează pe o analiză a riscului și o evaluare a impactului asupra protecției datelor, asigurându-se orientarea camerelor exclusiv către zonele cele mai importante dinăuntrul și din afara clădirilor.

Pentru a monitoriza punctele de intrare și ieșire ale incentei Spitalului, precum și ale tuturor clădirilor din incinta Spitalului sunt prevăzute camere de supraveghere. În plus, sunt prevăzute camere care monitorizează puncte de legătură, precum și proximitatea anumitor zone de importanță majoră care necesită o securizare suplimentară, cum ar fi zonele unde sunt păstrate sume de bani, unde se află aparatură performantă de investigație sau zone de acces restricționat. În principiu, nu se monitorizează zonele susceptibile să ofere un grad mai ridicat de discreție, cum sunt birourile sau saloanele.

4. TRANSFERURI IMAGINI SI ACCES IMAGINI

Imaginile rezultate din procesul de supraveghere video pot fi comunicate organelor judiciare sau de aplicare a legii pentru a ancheta sau urmări fapte penale. Aceste transferuri nu se efectuează decât la cerere, în baza unei solicitari scrise. Nu au loc transferuri periodice sau de rutină. De asemenea, persoanele care au suferit o pagubă materială în incinta spitalului pot solicita pe baza unei cereri scrise accesul la vizionarea înregistrărilor video relevante asupra faptei incriminate, în cazuri justificate, cum ar fi cele prevazute de legislație sau incidentele de securitate.
Angajații sau alte persoane interesate nu primesc acces la sistemul de supraveghere în alte scopuri decât cele menționate.
Persoanele vizate de supravegherea video au dreptul de a avea acces la datele personale pe care le deținem cu privire la acestea. Dacă se solicită în mod specific, se poate stabili o vizionare a imaginilor sau solicitantul poate obține o copie a imaginilor înregistrate. În cazul unei astfel de cereri, solicitanții trebuie să-și declare identitatea dincolo de orice bănuială (de ex, trebuie să aibă asupra sa documente de identitate la vizionare) și, ori de câte ori este posibil, să indice, de asemenea, data, timpul, locul și circumstanțele în care au fost filmați de cameră. Trebuie, de asemenea, să furnizeze o fotografie proprie recentă, care să permită personalului de securitate să-i identifice în imaginile analizate.

5. PROTEJAREA INFORMAȚIILOR

Pentru a proteja securitatea sistemului de supraveghere video ca întreg, inclusiv a datelor personale sunt puse în practică o serie de măsuri tehnice și organizaționale. Dintre aceste măsuri amintim:

- semnarea de acorduri cu subcontractanții care accesează date de natura personală;
- semnarea de către toți utilizatorii (externi și interni) a acordurilor de confidențialitate;
- limitarea duratei de stocare la 30 de zile;
- restricționarea accesului fizic la spațiile în care sunt amplasate dispozitivele DVR;
- acordarea drepturilor de acces pentru utilizatori numai la acele resurse care sunt strict necesare pentru ca aceștia să-și poată desfășura activitatea (pe baza necesității de a cunoaște).

6. FURNIZAREA INFORMAȚIILOR PRIVIND ZONELE SUPRAVEGHEATE

Respectăm dreptul persoanelor vizate la informare și furnizăm persoanelor vizate de prelucrări (care trec pe lângă perimetrul spitalului și/sau care intră în incinta spitalului) anunțuri cu privire la faptul că are loc o monitorizare și furnizăm informații cu privire la prelucrare. Modelul de informare este prezentat în continuare: