# POLITICA DE SECURITATE PRIVIND MĂSURILE DE PROTECȚIE A PERSOANELOR CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

## 1. DEFINIȚII

*„Regulamentul”* - Regulamentul (UE) 2016/679 al Parlamentului Eurpean 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, în limba engleză General Data Protection Regulation);

*„date cu caracter personal (date)”* - orice informații privind 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;

*„categorii speciale de date cu caracter personal”* – orice informație care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, date genetice, 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

*„sistem de evidență a datelor cu caracter personal”* - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice.

*„date anonime”* - reprezintă orice date ale căror origine sau în baza cărora au fost efectuate prelucrări, însă acestea nu pot fi asociate cu nicio persoană vizată identificată sau identificabilă;

*„prelucrarea datelor cu caracter personal (prelucrare)”* - înseamnă 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;

*„operator*” - 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;

*„persoană împuternicită de operator”* - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

*„persoană autorizată să prelucreze date (persoana autorizată)”* - Operatorul sau Împuternicitul sau persoanele care, sub autoritatea directă a Operatorului sau a Împuternicitului, sunt autorizate să prelucreze Date;

*„destinatar”* - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile 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 autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

*„parte terță”* - înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

*„consimțământ*” - al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

*„încălcarea securității datelor cu caracter personal”* - înseamnă o încălcare a securității care 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;

*„reprezentant”* - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;

*„reguli corporatiste obligatorii”* - înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

*„autoritate de supraveghere*” - înseamnă o autoritate publică independentă instituită de un stat membru;

*„DPO”* - responsabilului cu protecția datelor (în limba engleză, data protection officer);

*„DPIA”* - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA);

*„transmitere”* - înseamnă transmiterea în orice formă a datelor cu caracter personal spre a fi cunoscute și consultate de una sau mai multe părți;

*„persoana vizată”* - o persoană fizică identificabilă 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;

*„difuzare/divulgare”* - înseamnă aducerea la cunoștința uneia sau mai multor părți a datelor cu caracter personal, în orice formă, și de asemenea, punerea acestora la dispoziție spre a fi consultate;

*„restricționarea prelucrării*” - înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

*„creare de profiluri”* - înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia.

## 2. REFERINȚE NORMATIVE

- Declaraţia Universală a Drepturilor Omului;
- Carta Drepturilor Fundamentale a Uniunii Europene;
- 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);
- Regulamentul 2016/679/UE, 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;
- Legea nr. 682 din 28 noiembrie 2001 privind ratificarea Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981;
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;
- Legea 102/2005, modificată și completată, privind infiintarea, organizarea si functionarea Autoritatii Nationale de Supraveghere a Prelucrarii Datelor cu Caracter Personal;
- Legea 504/2002, a audiovizualului, cu completările şi modificările ulterioare;
- Decizia Consiliului Naţional al Audiovizualului nr. 220/2011, privind Codul de reglementare a conţinutului audiovizual, cu completările şi modificările ulterioare;
- Legea 8/1996, privind dreptul de autor şi drepturile conexe;
- Ordonanța Guvernului 39/2005 privind cinematografia cu modificările și completările ulterioare;
- Ordonanţa guvernului nr. 27/2002, privind reglementarea activităţii de soluţionare a petiţiilor;
- Decizia nr. 128/2018 privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 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;
- Directiva 2010/13/UE a Parlamentului European şi a Consiliului din 10 martie 2010 privind coordonarea anumitor dispoziţii stabilite prin acte cu putere de lege sau acte

administrative în cadrul statelor membre cu privire la furnizarea de servicii mass-media audiovizuale (Directiva serviciilor mass-media audiovizuale);

- Directiva 2016/680/CE, 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;
- Decizia nr. 133 din 3 iulie 2018 privind aprobarea Procedurii de primire şi soluţionare a plângerilor
- Decizia nr. 161 din 09 Octombrie 2018 privind aprobarea Procedurii de efectuare a investigaţiilor
- Decizia nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal
- Legea 477/2004 privind Codul de conduită al personalului contractual din autorităţile şi instituţiile publice;
- Legea 319/2006 privind sănătatea şi securitatea în muncă, cu modificările şi completările ulterioare;
- Legea nr. 333/2003, privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, cu modificările şi completările ulterioare;
- Hotărârea Guvernului nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor
- Legea 53/2003 - Codul Muncii,
- Legea 82/1991, actualizată – a contabilităţii
- Codul civil;
- Legea 95 / 2006 privind reforma în domeniul sănătății

## 3. SCOPUL ȘI DOMENIUL DE APLICABILITATE

### 3.1. Scopul

Prezenta Politică are drept scop stabilirea principiilor de bază a prelucrării datelor cu caracter personal, metodologia de lucru, precum și reguli pentru Angajați pentru a se asigura confidențialitatea datelor personale în operațiunile de prelucrare **a datelor personale** efectuate de Spitalul Clinic Județean de Urgență Cluj-Napoca („Spitalul", "SCJU Cluj-Napoca" sau „Operatorul"), în conformitate cu legislația aplicabilă.

Respectarea confidențialității datelor cu caracter personal reprezintă o obligație a Operatorului și a Angajaților săi, având în vedere sensibilitatea datelor cu caracter personal prelucrate, dreptul la protecția datelor personale și dreptul la viața privată a persoanelor fizice.

Angajații Operatorului înțeleg și au reprezentarea deplină a faptului că încălcarea confidențialității datelor personale poate conduce la prejudicii fizice, materiale sau morale persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

### 3.2. Destinatari

Prevederile prezentei Politici sunt obligatorii pentru angajații permanenți și temporari ai SCJU Cluj-Napoca, precum și pentru orice alte persoane care, deși nu sunt angajații Spitalului, pot fi asimilați unui personal dedicat Spitalului (de ex. voluntarii, studenții etc) (**toate aceste persoane fiind denumite în acest document în mod generic „Angajați"**).

Prezenta Politică va fi considerată ca având caracter general și se va aplica tuturor prelucrărilor efectuate de Operator. Acest document stabilește modul în care vor fi protejate datele personale pe care Operatorul le deține și le prelucrează în îndeplinirea activităților sale de furnizare servicii medicale.

În cazul în care se constată existența anumitor aspecte legate de confidențialitate, pentru care prezenta Politică nu oferă directive corespunzătoare, Angajații trebuie să solicite imediat consiliere din partea Ofițerului responsabil cu protecția datelor (DPO) numit, sau a reprezentantului legal al Operatorului.

### 3.3. Sfera datelor personale

#### 3.3.1.Datele pacienților

Operatorul prelucrează următoarele date cu caracter personal aparținând pacienților și/sau celorlalte Persoane Vizate (de ex: aparținătorii pacienților):

a). pentru furnizarea serviciilor medicale, gestionarea sistemelor și serviciilor de sănătate, decontarea serviciilor medicale de sănătate de către CAS/DSP, realizarea de cercetări științifice și pentru prelucarea statistică a datelor:

1. nume, prenume, adresa de domiciliu, adresa de reședință, cetățenia, cod numeric personal, seria şi numărul actului de identitate;
2. setul minim de date la nivel de pacient, reglementate prin Ordinul nr. 1782/2006 anexele 6 şi 7 aferente spitalizării continue și spitalizării pe zi, ca de exemplu, fără a se limita la, codul de identificare al asiguratului, sexul, data nașterii, domiciliul, cetățenia, ocupația și nivelul de instruire, număr card european, număr card național, diagnostic la externare, starea la externare, proceduri medicale efectuate;
3. datele şi informaţiile medicale reglementate prin ordinul nr. 1123/849/2016 anexa 2 din dosarul electronic de sănătate (ca de exemplu, fără a se limita la, datele menționate la punctul 2 de mai sus, simptome, istoricul medical, istoricul de îngrijire, mod de viață, tratament, servicii și investigații clinice).

Operatorul va prelucra datele mai sus menționate pentru gestionarea sistemelor și serviciilor de sănătate. În acest sens, pentru a asigura servicii medicale de cea mai bună calitate, Spitalul va prelucra datele în scopul organizării gărzilor, raportărilor, realizarea evidenței serviciilor medicale, arhivării foilor de observație clinică generală, fișelor de spitalizare de zi/imagistică, întocmirii fișelor de consum, controlul accesului vizitatorilor în saloanele Spitalului, etc.

b). pentru întocmirea documentelor fiscale și încasarea contravalorii Serviciilor medicale de la pacienții care nu sunt asigurați sau beneficiază de Servicii medicale nedecontate de CAS sau, după caz, încasarea coplății, se prelucrează: numele, prenumele și adresa de domiciliu.

c). în scopul îmbunătățirii serviciilor medicale (cum ar fi completarea Chestionarului pentru evaluarea gradului de satisfacție a pacientului) se prelucrează date precum: numărul de telefon și adresa de email.

d). colectează și prelucrează datele – imaginea - în scopul asigurării securității bunurilor și a persoanelor prin intermediul supravegherii video existentă în spațiile publice.

e). pentru soluționarea de cereri, întrebări și/sau reclamații ale persoanelor fizice, se prelucrează date precum: nume, prenume, adresa de comunicare și/sau email, număr de telefon.

Spitalul poate colecta și utiliza datele personale ale pacienților (de exemplu: nume, vârsta, data nașterii, adresa, rezidența, e-mail etc.), pentru formularea de acțiuni/apărări juridice și pentru furnizare de informații și documente în proceduri/investigații/cereri în raport cu autorități/instituții/alte entități competente legal. De asemenea, dacă în viitor decide să prelucreze datele cu caracter personal ale pacienților în scopul promovării Spitalului, prin utilizarea de fotografii/înregistrări video, prin intermediul unor canale diferite de comunicare (de exemplu, fără a se limita la, website, mass-media, facebook etc.), după obținerea consimțământului acestora, poate prelucra date precum: imaginea captată de fotografii/înregistrările video.

### 3.3.2.Datele angajaților și ale persoanelor asimilate acestora

SCJU Cluj-Napoca colectează și utilizează datele personale ale angajaților săi (actuali și foști) în cadrul desfășurării raporturilor de muncă/contractelor de colaborare inclusiv a obligațiilor care decurg din acestea, în temeiul legii și numai în scopuri relevante, corespunzătoare și uzuale. Departamentul Resurse Umane va comunica Angajaților informații în legătură cu motivele și metodele de prelucrare a datelor respective.

Astfel, în conformitate cu legislația aplicabilă și implicit a gestionării dosarelor de concurs în diferitele etape ale procedurilor de angajare, pentru încheierea și executarea CIM SCJU Cluj-Napoca prelucrează datele după cum urmează: nume și prenume, adresă de domiciliu, data și locul nașterii, cetățenia, cod numeric personal, seria și numărul cărții de identitate, pașaportului sau a altui act de identitate, semnătura, profesia, locul de muncă, formarea profesională (diplome, studii), date conținute de diplome sau alte documente care atestă îndeplinirea condițiilor specifice ale postului, expertiza lingvistică, niveluri de competențe; date privind cazierul judiciar; informații și date din CV (nume, prenume, adresă, e-mail, număr telefon, vârstă, data nașterii (opțional), sex, fotografie (opțional), stare civilă (opțional), naționalitate (opțional), experiență profesională, studii și/sau calificări profesionale) date privind starea de sănătate conținute de adeverința medicală care atestă starea de sănătate; adresa de e-mail și numărul de telefon; conturile bancare, imaginea angajaților înregistrată de camerele de supraveghere video amplasate în locuri publice în Spital, codul de parafă, funcţie, specialitate medicală, dată început specialitate, competenţe, date legate de semnătură electronică, precum și alte date ce derivă din specificul activității Spitalului ca furnizor de servicii medicale.

Spitalul recunoaște și respectă drepturile de confidențialitate ale angajaților săi, limitând colectarea, accesul și utilizarea datelor personale aferente angajării. SCJU Cluj-Napoca ia măsuri preventive suplimentare înainte de divulgarea către părțile terțe legitime a informațiilor oricărui angajat. Respectivele divulgări pot avea loc numai în condițiile în care există înțelegerea deplină a faptului că accesul și utilizarea datelor sunt limitate, și că datele trebuie să fie protejate.

În unele cazuri, este posibil să fie solicitate date conținute în cazierul judiciar, inclusiv situația litigiilor în care angajatul este implicat, acestea fiind necesare Operatorului pentru evaluarea angajaților și/sau garanțiilor pe care le prezintă aceștia. Numai după obținerea consimțământului, în scopul promovării SCJU Cluj-Napoca, prin utilizarea de fotografii/înregistrări video cu angajații, prin intermediul unor canale diferite de comunicare

(de exemplu, fără a se limita la website, mass-media, facebook etc.), poate prelucra datele cu caracter personal după cum urmează: imaginea captată de fotografii/înregistrările video.

## 4. PRINCIPII GENERALE

### 4.1. Soluțiile de organizare

SCJU Cluj-Napoca, în calitate de Operator, a adoptat următoarele soluții de organizare în ceea ce privește confidențialitatea datelor:

- aspectele tehnice de securitate a datelor intră în responsabilitatea Birou informatică, GamaIT (platforma ATLAS MED), societatea Info World S.R.L. (platformele SALARY MANAGEMENT și PONTAJEPLUS) și trebuie gestionate atât în baza liniilor directoare definite, a proceselor și procedurilor, cât și prin controale efectuate la nivelul sistemelor informatice;
- responsabilitatea privind prelucrarea datelor în acord cu prezenta politică revine tuturor Angajaților. Operatorul va asigura măsurile organizatorice necesare implementării prevederilor Regulamentului și Politicii privind confidențialitatea datelor, astfel încât prelucrările datelor cu caracter personal să fie efectuate în conformitate cu Regulamentul (UE) 2016/679;
- fără prejudicierea celor de mai sus, Operatorul desemnează un Responsabil cu protecția datelor care va supraveghea toate activitățile de prelucrare a datelor personale.
- Responsabilul cu protecția datelor se va asigura că angajații Spitalului au acces la informația necesară respectării confidențialității datelor personale prelucrate și mecanismele de asigurare a confidențialității;

Angajații Spitalului sunt obligați să respecte Politica de confidențialitate precum și măsurile de prelucrare a datelor cu caracter personal, asigurând-se un nivel adecvat de protecție a datelor astfel prelucrate.

### 4.2. Prevederi generale

Desfășurarea activității curente a SCJU Cluj-Napoca presupune efectuarea de către Angajații Spitalului a unor prelucrări de date care se supun următoarelor principii:

- datele trebuie prelucrate în mod legal, echitabil și transparent;
- datele trebuie colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale;
- datele trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- datele trebuie să fie exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;
- datele trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal vor fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;

- datele trebuie prelucrate într-un mod care asigură securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

Prin măsurile adoptate, operatorul se angajează să implementeze măsurile tehnice și organizatorice necesare asigurării gradului de confidențialitate necesar și securității prelucrării datelor cu caracter personal.

Datele personale vor putea fi colectate, folosite, reținute, transmise și șterse, respectându-se confidențialitatea conținutului acestora, precum și celelalte reguli stabilite în prezenta Politică precum și obligațiile prevăzute în cadrul Regulamentului.

### 4.3. Securitatea prelucrării

Asigurarea securității prelucrării datelor cu caracter personal implică respectarea unui nivel adecvat al confidențialității datelor și se va face cu respectarea de către Operator a măsurilor tehnice și organizatorice precum:

- ✓ pseudonimizarea și criptarea datelor cu caracter personal;
- ✓ capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- ✓ capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- ✓ implementarea unor procese pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Operatorul se va asigura că principiile de mai sus sunt respectate. De asemenea, acesta trebuie să poată dovedi respectarea principiilor și îndeplinirea obligațiilor ce decurg din acestea.

Accesul Angajaților la datele personale deținute va fi acordat în baza unei autorizații corespunzătoare, în funcție de grupul din care fac parte aceștia și de nivelul de securitate la care este arondat. Orice Angajat/Parte terță autorizată/Destinatar care va avea acces la datele personale deținute de Operator doar ca urmare a necesității de a utiliza informațiile respective, va avea obligația de a respecta confidențialitatea acestora și de a respecta măsurile tehnice și organizatorice astfel încât datele prelucrate să fie protejate. În acest sens, activitatea angajaților SCJU Cluj-Napoca va putea fi monitorizată pentru a se verifica respectarea conformității cu legile sau normele în vigoare, de protecție a datelor personale și cu Politicile de protectie a datelor, implementate.

În cazul în care există suspiciunea încălcării prezentei Politici de confidențialitate, incidentul trebuie raportat cel puțin uneia dintre persoanele următoare:

- ✓ Coordonatorilor secțiilor/compartimentelor/laboratoarelor/serviciilor/birourilor;
- ✓ Ofițerului responsabil de protecția datelor;
- ✓ Managerului SCJU Cluj-Napoca.

Aceștia din urmă sunt obligați să ia măsurile necesare conform regulilor legale sau celor stabilite în procedurile de raportare și tratare incidente la nivelul Spitalului.

### 4.4. Reguli privind prelucrarea datelor

a) Legalitatea - Prelucrarea datelor cu caracter personal se face în temeiul şi în conformitate cu prevederile legale;

b) Confidenţialitatea - Persoanele care prelucrează date cu caracter personal au prevăzută în *Contractul individual de muncă* şi în *Fişa postului* o clauză de confidenţialitate şi completează *Declaraţia de confidenţialitate*.

c) Consimţământul persoanei vizate - Orice prelucrare de date cu caracter personal, cu excepţia prelucrărilor care vizează date din categoriile strict menţionate în Regulamentul nr. 679/27.04. 2016 şi în Legea 190/2018, poate fi efectuată numai dacă persoana vizată şi-a dat consimţământul în mod expres şi neechivoc pentru acea prelucrare;

d) Informarea - Informarea persoanelor se face de către instituţia care intră prima în contact direct cu persoana vizată, respectiv pentru angajaţi /candidaţi /participanţi la proiecte iniţiate sau de Instituţiile cu care colaborează – pentru persoanele vizate implicate de respectivele Instituţii; De asemenea, pe prima pagină a website-ului Instituţiei va fi introdusă NOTA DE INFORMARE.

e) Protejarea persoanelor vizate - Persoanele vizate au mai multe drepturi, conform regulamentului 679/2016, respectiv d**reptul de a fi informat, dreptul de acces la date, dreptul la rectificare a datelor, d**reptul la ştergerea datelor ("dreptul de a fi uitat"), dreptul la restricţionarea prelucrării, dreptul de a fi notificat privind rectificarea sau ştergerea datelor cu caracter personal sau restricţionarea prelucrării, dreptul la portabilitatea datelor, dreptul la opoziţie, dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri precum şi dreptul de a se adresa Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal sau instanţei de judecată pentru apărarea oricăror drepturi garantate de lege, care le-au fost încălcate;

f) Securitatea - Măsurile sunt stabilite astfel încât să asigure un nivel adecvat de securitate cu ocazia prelucrării datelor cu caracter personal;

g) Prelucrarea datelor cu caracter personal, letric sau electronic, se efectuează de către personalul responsabil din cadrul instituției, conform fişei postului.

h) Documentele se înregistrează şi manipulează potrivit regulilor generale de gestionare a documentelor ordinare.

1. Nici o prelucrare de date cu caracter personal nu poate fi efectuată fără consimţământul persoanei vizate, cu excepţia următoarelor situaţii:

a. când prelucrarea este necesară în vederea protejării vieţii, integrităţii fizice sau sănătăţii persoanei vizate ori a unei alte persoane ameninţate;

b. când prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale a instituției ;

c. când prelucrarea este necesară în vederea exercitării prerogativelor de autoritate publică cu care este învestit operatorul sau terţul căruia îi sunt dezvăluite datele;

d. când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele, cu condiţia ca acest interes să nu prejudicieze interesul sau drepturile şi libertăţile fundamentale ale persoanei vizate;

e. când prelucrarea este făcută exclusiv în scopuri statistice iar datele rămân anonime pe toată durata prelucrării.

2. Categoriile de destinatari ai datelor cu caracter personal prelucrate de către SCJU Cluj-Napoca sunt:

a. Persoana vizată (candidatul/ angajatul/cetăţeanul);
b. Autorităţi publice centrale;
c. Organismele de asigurare a calităţii
d. Instituţii abilitate să efectueze verificări asupra activităţii SCJU Cluj-Napoca;
e. Instituţii de învăţământ partenere;
f. Inspectoratul Teritorial de Muncă;
g. Instituţii bancare;

h. Casa Naţională de Asigurări Sociale;
i. Servicii de sănătate publică (CNAS, casele de sănătate judeţene);
j. Casa Naţională de Pensii Publice;
k. Poliţie, Parchet, Instanţe;
l. Instituţii către care persoana vizată solicită portarea datelor cu caracter personal;

**4.5. Sursele de risc privind accesul la datele cu caracter personal a unor persoane neautorizate:**

i. Potenţiala dezordine în care sunt lăsate/folosite materiale ce conţin date cu caracter personal;
ii. Lăsarea pe birouri a unor documente ce conţin date cu caracter personal şi părăsirea încăperii, fără a încuia uşa, în situaţia în care cel ce a plecat este singurul ocupant sau ultimul care pleacă;
iii. Utilizarea neautorizată, în interiorul birorilor în care se folosesc materiale ce conţin date cu caracter personal, a aparaturii foto sau de înregistrare video, incluzând aici, dar nelimitativ, dispozitive mobile de tip smartphone sau tablete;
iv. Depozitarea materialelor ce conţin date cu caracter personal în spaţii neasigurate corespunzător;
v. Pătrunderea în clădirile SCJU Cluj-Napoca a unor persoane rău intenţionate, indiferent de oră;
vi. Prezenţa vreunei persoane rău intenţionate într-una dintre incăperi şi sustragerea unor documente ce conţin datele cu caracter personal, în format letric sau electronic, din dosare sau de pe computer;
vii. Efectuarea neautorizată de copii de pe documentele ce conţin date cu caracter personal;
viii. Depozitarea materialelor ce conţin date cu caracter personal pe medii de stocare neasigurate / neautorizate;
ix. Conectarea unor medii de stocare neasigurate / neautorizate la staţiile de lucru IT (Desktop sau Laptop);
x. Transportarea documentelor ce conţin date cu caracter personal în condiţii improprii acestei activităţi, existând riscul de a fi pierdute/de a fi sustrase unele dintre acestea datorită neatenţiei sau grabei celui care le transportă;
xi. Lăsarea staţiilor de lucru IT pe care sunt prelucrate date cu caracter personal, în funcţiune, fără a limita accesul la consola de lucru, atunci când se părăseşte încăperea de singurul ocupant sau de ultimul care pleacă, fără a se încuia uşa;
xii. Lăsarea în funcţiune a aparaturii IT la finalul programului de lucru;
xiii. Accesul publicului în interiorul spaţiului de lucru al angajaţilor, putându-se vedea ecranele staţiilor de lucru IT sau conţinutul documentelor de pe birouri;
xiv. Utilizarea de persoane neautorizate a staţiilor de lucru IT pe care sunt stocate date cu caracter personal;
xv. Modificarea neautorizată a setărilor staţiilor de lucru IT, astfel încât să poată fi folosite de oricine;
xvi. Folosirea la prelucrarea datelor cu caracter personal de către angajaţii autorizaţi ai Primăriei, a unor staţii de lucru IT care nu aparţin Instituţiei;
xvii. Instalarea pe staţiile de lucru IT a unor programe pentru care SCJU Cluj-Napoca nu deţine licenţă de utilizare;

xviii. Instalarea pe staţiile de lucru IT a unor programe ce permit accesul/utilizarea de la distanţă şi/sau activarea funcţiilor de lucru la distanţă preexistente în sistemele de operare (ex. RDP) în mod neautorizat;

xix. Scoaterea din Instituţie a unor staţii de lucru IT (Desktop sau Laptop) pe care sunt stocate date cu caracter personal;

xx. Utilizarea de către angajaţi a adreselor de e-mail personale, create în alte domenii decât cel ce aparţine SCJU Cluj-Napoca.

### 4.6. Solicitarea accesului la date

O persoană vizată are drept de acces la datele cu caracter personal colectate care o privesc şi poate să îşi exercite acest drept cu uşurinţă şi la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare şi pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la datele lor.

Aşadar, are dreptul de a cunoaşte şi de a i se comunica în special scopurile în care sunt prelucrate datele, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal şi consecinţele unei astfel de prelucrări.

Dacă acest lucru este posibil, SCJU Cluj-Napoca trebuie să poată furniza acces de la distanţă la un sistem sigur, care să ofere persoanei vizate acces direct la datele sale cu caracter personal.

Acest drept nu ar trebui să aducă atingere drepturilor sau libertăţilor altora, inclusiv secretului comercial sau proprietăţii intelectuale şi, în special, drepturilor de autor care asigură protecţia programelor software.

Cu toate acestea, consideraţiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informaţiile persoanei vizate.

Având în vedere că SCJU Cluj-Napoca prelucrează un volum mare de informaţii privind persoana vizată, poate solicita ca, înainte de a îi fi furnizate informaţiile, persoana vizată să precizeze informaţiile sau activităţile de prelucrare la care se referă cererea sa.

Dreptul de ştergere a datelor aparţinând persoanelor vizate **nu se aplică** dacă SCJU Cluj-Napoca prelucrează date cu caracter personal în baza sarcinii publice.

Persoana vizată are dreptul de a obține ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar SCJU Cluj-Napoca va avea obligația de a șterge datele fără întârzieri nejustificate în cazul în care s-a efectuat prelucrare de date cu alt scop, în afara celui cu care este investit în interes public iar persoana vizată și-a dat consimțământul, respectiv:

- datele nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea;
- datele cu caracter personal au fost prelucrate ilegal în alt scop;
- persoana vizată își exercită dreptul la opoziție în condițiile Regulamentului General pentru Protecția Datelor;
- datele trebuie șterse pentru respectarea unei obligații legale a operatorului;
- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii minorilor, în condițiile Regulamentului General pentru Protecția Datelor;

SCJU Cluj-Napoca, în calitate de operator de date, poate refuza cererea de ștergere a datelor în următoarele condiții:

- prelucrarea este necesară pentru exercitarea dreptului la liberă exprimare și la informare;

- prelucrarea este necesară pentru respectarea unei obligații legale aplicabile operatorului;
- prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în condițiile Regulamentului General pentru Protecția Datelor, în măsura în care exercitarea dreptului poate face imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective;
- prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Persoana vizată are dreptul de a obține din partea SCJU Cluj-Napoca, în calitate de operator de date, restricționarea prelucrării în următoarele cazuri:

- persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
- prelucrarea este ilegală, dar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
- SCJU Cluj-Napoca nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță;
- persoana vizată s-a opus prelucrării, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

Dreptul la portabilitatea datelor aparţinând persoanelor vizate **nu se aplică** dacă sunt prelucrate date cu caracter personal în baza sarcinii publice.

Ţinând cont de aceste aspecte, SCJU Cluj-Napoca foloseşte modelele de Cereri din de pe web-site-ul www.dataprotection.ro.

Orice cerere scrisă prin care o persoană solicită informaţii despre datele cu caracter personal care o privesc sau despre datele cu caracter personal ale altei persoane pe care o reprezintă în mod legal, se depune la sediul SCJU Cluj-Napoca şi se înregistrează la Secretariat, prezentându-se managerului, pentru a dispune măsurile ce se impun.

Având în vedere activitatea SCJU Cluj-Napoca, în situaţia în care angajatul care înregistrează corespondenţa nu poate încadra o solicitare, responsabilul cu protecţia datelor cu caracter personal stabileşte dacă solicitarea se încadrează în categoria *"cereri de acces la date cu caracter personal"* şi prezintă managerului propunerile pentru soluţionarea cererii;

O cerere de acces la date cu caracter personal trebuie să fie scrisă, datată şi semnată de persoana vizată sau de persoana care o reprezintă legal;

Orice cerere care îndeplineşte condiţiile prevăzute de lege va fi soluţionată.

Determinarea naturii juridice a solicitării se face prin raportare la conţinutul acesteia, nefiind obligatorie menţionarea în cuprinsul acesteia a legii sau existenţa titulaturii specifice ori indicarea în mod expres a dreptului a cărui exercitare se urmăreşte;

Informaţii necesare pentru soluţionarea cererii:

a. date referitoare la persoana vizată:
    i. numele şi prenumele, dacă este cazul - numele purtat anterior;
    ii. adresa de domiciliu/reşedinţă;
    iii. Codul numeric personal/Codul naţional de identificare;
    iv. telefon, în scopul asigurării comunicării (opţional);
    v. e-mail, în scopul asigurării comunicării (opţional);
b. scurtă descriere a situaţiilor care au presupus prelucrarea de date cu caracter personal;

c. dacă este cazul, numele, prenumele şi adresa reprezentantului legal, precum şi dovada mandatului;
d. dovada identităţii persoanei vizate/reprezentantului legal, în mod similar celor de la litera „a").

Verificarea identităţii persoanei vizate sau a reprezentantului legal este obligatorie şi se face prin verificarea directă la sediul SCJU Cluj-Napoca unde este depusă cererea de solicitare a datelor cu caracter personal, caz în care angajatul care va prelua cererea va confirma identitatea persoanei vizate pe baza confruntării cu documentele de identitate furnizate.

Verificarea identităţii solicitantului este necesară în scopul:

a. obţinerii dovezii certe a identităţii solicitantului,
b. obţinerii dovezii certe a relaţiei dintre solicitant si persoana vizată, acolo unde cererea se face în numele persoanei vizate,
c. protejării datelor cu caracter personal împotriva unui acces neautorizat sau ilegal,
d. asigurării persoanei vizate că operatorul ia toate măsurile tehnice si organizatorice pentru a asigura securitatea şi confidenţialitatea datelor cu caracter personal.

Certificarea identităţii se face pe baza actului de identitate, sau a paşaportului.

Orice persoană vizată are dreptul de a obţine de la operator, la cerere şi în mod gratuit pentru o solicitare pe an confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta.

SCJU Cluj-Napoca este obligat, în situaţia în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea şi drepturile pe care persoana vizată le are.

În cazul în care cererea nu îndeplineşte condiţiile prevăzute de lege, persoanei care a cerut informaţiile i se comunică motivele care au stat la baza neîndeplinirii celor solicitate.

SCJU Cluj-Napoca comunică informaţiile solicitate în termen de 30 zile de la data primirii cererii.

În măsura în care pentru soluţionarea cererii este necesară consultarea log-urilor, acestea sunt consultate de îndată, cel mai târziu în 48 de ore de la înregistrarea cererii, de administratorul de reţea.

Elaborarea răspunsurilor ce conţin date cu caracter personal, se va face de către angajatul structurii căruia i-a fost repartizat spre soluţionare, cu menţiunea „*Confidenţial ! Date cu caracter personal prelucrate în conformitate cu prevederile Regulamentului 679/2016* ". Documentul va fi semnat de cel care l-a elaborat, de către şeful structurii şi manager . Conţinutul răspunsului nu va face referire decât la solicitările petentului, fără a furniza date cu caracter personal suplimentare.

Trimiterea răspunsului se va face letric, la adresa de domiciliu sau, după caz, la adresa indicată de petent ori adresa de la care a fost înaintată solicitarea, cu menţiunea „*A se înmâna personal !!!* ".

Cererile de acces la datele cu caracter personal vor fi păstrate de către personalul din cadrul SCJU Cluj-Napoca căruia i-a fost repartizat spre soluţionare într-o mapă distinctă, care conţine următoarele documente, fără a se limita la acestea:

a. copii ale corespondenţei dintre operator şi persoana vizată;
b. evidenţa deciziilor luate de operator şi modul prin care s-au luat aceste decizii (acolo unde este cazul).

Registrul cererilor de acces va cuprinde cel puţin următoarele:

a. data la care a fost primită cererea,

b. numele şi prenumele persoanei vizate,
c. numele şi prenumele solicitantului, dacă este diferit de persoana vizată;
d. cine a întocmit răspunsul;
e. data transmiterii răspunsului;

Registrul cererilor de acces se păstrează la Secretariatul SCJU Cluj-Napoca şi este utilizat doar în scopul monitorizării numărului de cereri care au fost adresate operatorului, a persoanelor care au solicitat accesul, astfel încât să fie asigurată exercitarea dreptului de acces gratuit o dată pe an, precum şi a costurilor implicate.

În vederea apărării drepturilor prevăzute de Regulamentul 679/2016, persoanele ale căror date cu caracter personal au făcut obiectul unei prelucrări neautorizate pot înainta plângere către Autoritatea Naţională.

Autoritatea Naţională poate investiga, din oficiu sau la primirea unei plângeri, orice încălcare a drepturilor persoanelor vizate, respectiv a obligaţiilor care revin operatorilor şi, după caz, persoanelor împuternicite, în cadrul efectuării prelucrărilor de date cu caracter personal, în scopul apărării drepturilor şi libertăţilor fundamentale ale persoanelor vizate.

În exercitarea atribuţiilor de investigare, Autoritatea naţională poate solicita operatorului orice informaţii legate de prelucrarea datelor cu caracter personal şi poate verifica orice document sau înregistrare referitoare la prelucrarea de date cu caracter personal.

Secretul de stat şi secretul profesional nu pot fi invocate pentru a împiedica exercitarea atribuţiilor acordate Autorităţii de supraveghere. Atunci când este invocată protecţia secretului de stat sau a secretului profesional, Autoritatea naţională are obligaţia de a păstra secretul.

## 5. OBLIGAȚII GENERALE

Operatorul este obligat ca, în desfășurarea activităților sale medicale, să procedeze cu prudență, să respecte legislația României, să-și protejeze pacienții și celelalte Persoane Vizate, precum și propriile drepturi și interese.

Operatorul colaborează strâns cu toate secțiile, compartimentele, laboratoarele, serviciile și birourile aflate în subordinea sa.

Angajații Spitalului sunt obligați să asigure confidențialitatea datelor cu caracter personal în baza Contractului de muncă încheiat și a prezentei Politici de confidențialitate. Nerespectarea Politicii de confidențialitate sau a Contractului de muncă încheiat poate conduce către demararea unor acțiuni disciplinare, inclusiv la desființarea contractului de muncă.

Operatorul își rezervă toate drepturile de a proceda la recuperarea sumelor de bani acordate cu titlu de despăgubire unei persoane vizate, ca urmare a nerespectării de către angajați a Politicii de confidențialitate. Nerespectarea confidențialității datelor cu caracter personal prelucrate poate fi sancționată penal potrivit reglementărilor legale din materie.

Fiecare secție, compartiment, laborator, serviciu, birou din cadrul SCJU Cluj-Napoca are obligația păstrării unei evidențe (întocmire și actualizare) a persoanelor desemnate de Spital să prelucreze datele cu caracter personal, dacă prin natura activităților desfășurate în cadrul secției, compartimentului, laboratorului, serviciului, biroului este necesară prelucrarea de date cu caracter personal.

Prin prezenta Politică se stabilește faptul că managementul Spitalului are atribuția să supravegheze prelucrarea datelor, inclusiv buna funcționare a sistemelor informatice utilizate în activitatea de prelucrare și transmitere a datelor cu caracter personal. În exercitarea acestei atribuții, se poate solicita oricărui Angajat informații cu privire la prelucrarea datelor și se pot stabili, prin instrucțiuni de lucru, reguli obligatorii în domeniul prelucrării datelor.

Orice contract încheiat între SCJU Cluj-Napoca, în calitate de Operator de date cu caracter personal, și o terță parte, în calitate de Persoană Împuternicită, va trebui să cuprindă clauzele de confidențialitate și prelucrare a datelor cu caracter personal în conformitate cu Regulamentul.

### 5.1. Verificarea corectitudinii datelor cu caracter personal

Toți angajații au obligația să verifice datele personale păstrate de Spital din perspectiva acurateței și integralității informațiilor relevante și trebuie să le modifice corespunzător. Ca regulă generală, accesul este limitat la datele utilizate pentru identificarea unei persoane și nu include toate informațiile pe care Spitalul le păstrează despre Angajat.

De exemplu, SCJU Cluj-Napoca poate permite accesul la formularul de evaluare a performanței și la rezultatele individuale în cadrul planului de dezvoltare, însă informațiile generale ale planului de avansare vizând mai multe persoane nu pot fi împărtășite.

### 5.2. Activități personale

Angajamentul Spitalului de a respecta drepturile de confidențialitate ale Angajaților nu reprezintă permisiunea de a desfășura activități personale necorespunzătoare în timpul serviciului (ex. calculatoarele SCJU Cluj-Napoca trebuie să fie utilizate doar în interes de serviciu, sub nicio formă nu trebuie folosite în scopuri personale). În plus, pentru a asigura securitatea și protecția sistemelor sale IT, Spitalul are dreptul de acces în toate secțiile, compartimentele, laboratoarele, serviciile, birourile și, dacă este necesar, de a revizui comunicările și informațiile create de Angajați în timpul activității, în limitele permise de legislația în vigoare.

### 5.3. Refuzul de prelucrare a datelor cu caracter personal

Orice angajat are dreptul de a transmite departamentului Resurse Umane obiecțiuni în legătură cu colectarea, utilizarea și divulgarea datelor sale personale. SCJU Cluj-Napoca va evalua obiecțiunile Angajatului, va lua o decizie în conformitate cu legislația în vigoare și va comunica decizia sa Angajatului.

### 5.4. Transmiterea de informații

Spitalul va transmite datele legate de angajații și pacienții săi, structurilor aflate în subordine, doar dacă este necesar sau, dacă este posibil, în conformitate cu legea aplicabilă. Aceste structuri vor adopta orice măsuri de precauție menite să asigure legalitatea comunicării și respectării „secretului profesional".

Transmiterea în cadrul secțiilor/compartimentelor/laboratoarelor/serviciilor/birourilor Operatorului a datelor referitoare la pacienții/angajații SCJU Cluj-Napoca este permisă, cu titlu de exemplu, în următoarele cazuri:

- ✓ atunci când interesele părților sunt echilibrate: transmiterea este permisă, în scopuri de colaborare cu alți specialiști, în conformitate cu prevederile art. 28 din Codul de deontologie medicală: în situația în care pacientul a fost preluat sau îndrumat către un alt specialist, medicul va colabora cu acesta din urmă, punându-i la dispoziție orice fel de date sau informații cu caracter medical referitoare la persoana în cauză și informându-l cu privire la orice altă chestiune legată de starea de sănătate a acesteia. Pe cale de consecință, numai personalul medical care s-a ocupat de tratarea/diagnosticarea pacientului sau urmează să preia pacientul, are dreptul de a transmite și a primi asemenea date personale; transmiterea este permisă, în scopuri de plată a salariilor, în situația în care departamentul RUNO

transmite datele angajaților departamentului Salarii pentru ca acesta din urmă să poată efectua plata salariului în contul bancar al angajatului; când este necesar a se realiza alte activități în interes de serviciu.

✓ date anonime (de ex. în scopuri statistice sau în scopuri științifice).

Transmiterea datelor referitoare atât la pacienți, cât și la angajați este permisă, cu titlu de exemplu, în următoarele cazuri:

✓ **când există consimțământul expres al persoanelor vizate**: consimțământul trebuie să fie specific și astfel, strict legat de obiectul pentru care respectiva transmitere este efectuată (ex. promovare). Pe cale de consecință, pentru ca, Spitalul să se asigure că acceptul a fost acordat legitim de către pacient/angajat, este necesară verificarea conținutului notificării de informare trimise persoanei vizate și formularul de consimțământ aferent.

✓ **cazurile care sunt echivalente consimțământului**: (ex. încheierea unui contract, obligație legală, interes legitim al Operatorului).

## 6. OBLIGAȚII SPECIFICE

Prelucrarea datelor cu caracter personal se face doar de către angajații Operatorului ce dețin competența necesară efectuări unei astfel de prelucrări. În situația în care angajatul nu cunoaște gradul său de acces la date confidențiale, se va putea adresa managerului/DPO ului/coordonatorului secției/compartimentului/laboratorului/serviciului/biroului din care acesta face parte.

În vederea menținerii confidențialității adecvate a datelor cu caracter personal, Angajații sunt obligați să respecte restricțiile de procesare a datelor impuse de Operator prin Procedura de sistem privind asigurarea securității datelor cu caracter personal (PS-07) implementată, în funcție de categoria datelor și nivelul de acces.

SCJU Cluj-Napoca utilizează măsuri corespunzătoare din punct de vedere administrativ, tehnic, fizic și de securitate, menite:

(i) să respecte cerințele legale și acordurile de muncă;

(ii) să protejeze datele cu caracter personal împotriva pierderilor, furtului, accesului neautorizat, utilizării sau modificării.

Spitalul utilizează toate mijloacele necesare pentru a păstra datele personale corecte, complete și actualizate.

### 6.1. Drepturile persoanelor vizate

GDPR conferă persoanelor fizice, în principal, următoarele drepturi:

- Dreptul de a fi informat
- Dreptul de acces
- Dreptul la rectificare
- Dreptul de ștergere
- Dreptul de a restricționa prelucrarea
- Dreptul la portabilitatea datelor
- Dreptul de a se opune
- Dreptul legat de luarea de decizii automatizate și de profilare.

### 6.2. Transferul

Modalitatea prin care SCJU Cluj-Napoca transferă date cu caracter personal, în conformitate cu Regulamentul, respectiv toate operațiunile de transfer se vor face respectându-se Politica privind schimbul de date cu caracter personal, implementată la nivelul Spitalului.

### 6.3. Reținerea și ștergerea datelor personale

Reținerea datelor cu caracter personal reprezintă o prelucrare a datelor cu caracter personal în sensul Regulamentului. Reținerea datelor cu caracter personal se va efectua doar în situația în care operatorul a identificat unul dintre temeiurile legale prevăzute de Regulament pentru o anumită categorie de date personale, în conformitate cu Procedura de sistem privind asigurarea securității datelor cu caracter personal PS-07.

#### 6.3.1. Forma datelor reținute

*Format electronic*

Datele personale vor fi reținute în format electronic, cu respectarea măsurilor tehnice și organizatorice prevăzute în Politica de confidențialitate. Datele cu caracter personal vor fi păstrate într-o formă care să permită identificarea persoanelor vizate, pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. În cazul în care scopul prelucrării datelor nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu va păstra informații suplimentare necesare identificării persoanei vizate, în scopul unic al respectării drepturilor persoanelor vizate.

*Format fizic*

Datele prelucrate în format fizic vor reprezenta date personale în acord cu prevederile Regulamentului, în măsura în care acestea fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor. Datele vor fi reținute cu respectarea măsurilor tehnice și organizatorice prevăzute în Politica de confidențialitate. Datele cu caracter personal vor fi păstrate într-o formă care să permită identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. În cazul în care scopul prelucrării datelor nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu va păstra informații suplimentare necesare identificării persoanei vizate în scopul unic al respectării drepturilor persoanelor vizate.

#### 6.3.2. Informații referitoare la datele personale reținute

*Reducerea la minimum a datelor*

SCJU CLUJ respectă principiul reducerii la minimum a datelor potrivit Regulamentului, respectiv reține și stochează numai datele relevante și necesare îndeplinirii scopului prelucrării, conform Politicii de confidențialitate.

*Exactitate*

Datele personale prelucrate de SCJU CLUJ sunt exacte și actualizate la momentul stocării, efectuând verificări pentru a asigura acest aspect, în cazul în care este necesar.

### 6.3.3. Termenele de stocare

SCJU CLUJ ia măsuri adecvate privind eliminarea datelor cu caracter personal atunci când acestea nu mai sunt necesare atingerii scopului prelucrării. Acest lucru reduce riscul stocării unor date inexacte, inutile sau irelevante. Această obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor.

La împlinirea termenelor prevăzute în Nomenclatorul Arhivistic, se va asigura ștergerea/distrugerea datelor personale, cu excepția cazului în care legislația EU sau cea națională prevăd obligația păstrării acestora pe o perioadă mai îndelungată, în scopuri statistice, de arhivare în interes public, de cercetare științifică sau istorică și cu asigurarea măsurilor tehnice și organizatorice adecvate, în vederea garantării drepturilor și libertăților persoanei vizate.

În aceste cazuri, datele prelucrate, al cărui timp de stocare s-a împlinit, vor putea fi arhivate cu respectarea măsurilor tehnice și organizatorice stabilite în Politica de confidențialitate.

### 6.3.4 Reguli privind ștergerea datelor cu caracter personal

La sfârşitul perioadei de reţinere, datele stocate trebuie să fie revizuite şi eliminate. Sistemele automate pot semnala momentul la care datele personale ar trebui revizuite sau şterse, după o perioadă de timp determinată.

- Distincție ștergere-arhivare

Există o diferență semnificativă între ștergerea definitivă și arhivarea datelor cu caracter personal. Dacă datele personale sunt arhivate, acest lucru ar trebui să le reducă disponibilitatea și riscul de pierdere, distrugere accidentală, alterare etc.

Datele personale vor fi arhivate atunci când există obligația de a fi păstrate în continuare.

Persoanelor vizate li se va permite exercitarea dreptului de acces la datele cu caracter personal și li se vor respecta principiile privind protecția datelor cu caracter personal, având în vedere faptul că arhivarea datelor reprezintă o prelucrare în conformitate cu dispozițiile Regulamentului.

Atunci când este necesar să fie şterse anumite date cu caracter personal, prelucrate în activitatea curentă a organizației, vor fi eliminate orice copii efectuate de pe acestea.

Ștergerea datelor personale presupune eliminarea/distrugerea acestora, precum și a oricăror copii existente.

Ștergerea datelor personale se efectează la momentul împlinirii termenelor stabilite în Nomenclatorul Arhivistic, precum și ori de câte ori datele stocate sunt inexacte și nu pot fi rectificate, persoana vizată și-a retras consimțământul prelucrării datelor cu caracter personal - cu excepțiile prevăzute de lege, sau stocarea acestora nu mai este necesară îndeplinirii scopului/scopurilor în care au fost prelucrate, cu respectarea procedurilor aferente acestor situații.

- Operațiunea de ștergere a datelor cu caracter personal

Ștergerea datelor cu caracter personal este una efectivă și reală, astfel încât conținutul lor să nu mai poată fi recuperat în niciun fel.

*Date în format electronic*

Spitalul va lua următoarele măsuri de ștergere a datelor cu caracter personal:

- printr-un program software de distrugere a datelor de pe hard-disk;
- prin contractarea unui furnizor de servicii IT specializat în operațiunile de ștergere a datelor;

SCJU CLUJ va lua următoarele măsuri de scoatere din uz a datelor cu caracter personal:

- păstrarea datelor personale într-un folder criptat și restricționat accesului, cu instituirea unor măsuri de securitate tehnice și organizatorice corespunzătoare;
- operatorul nu este în măsură și nu va utiliza datele cu caracter personal, ulterior scoaterii din uz;
- operatorul se angajează să șteargă definitiv datele personale, de îndată ce acest lucru devine posibil/este fezabil – după momentul scoaterii din uz.

Aceste măsuri se vor lua numai în situația în care datele nu pot fi șterse fără a elimina alte informații necesare activității Operatorului ce se regăsesc în aceeași partiție a Hard Disk-ului.

*Date în format fizic*

SCJU CLUJ va lua următoarele măsuri de ștergere a datelor cu caracter personal: prin utilizarea distrugătoarelor de hârtie;

- Măsuri organizatorice și tehnice în situația în care datele șterse sunt publice

În cazul în care datele șterse/care urmează să fie șterse, sunt publice, Operatorul va lua măsuri rezonabile pentru a informa ceilalți operatori care prelucrează date cu caracter personal, că persoana vizată a solicitat ștergerea a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale datelor cu caracter personal.

Operatorul va contacta ceilalți operatori care prelucrează datele personale, enumerând și identificând datele personale a căror ștergere se solicită de către persoana vizată, prin următoarele metode:

- prin intermediul e-mail-ului;
- prin intermediul fax-ului;
- prin intermediul serviciilor de curierat rapid;

Spitalul Clinic Județean de Urgență Cluj își rezervă dreptul de a modifica ulterior prezenta Politică de Prelucrare a Datelor (de ex., din cauza modificărilor legislative și de practică în materie, ori a modificărilor în activitățile noastre). Prezenta Politică se completează cu alte politici specifice în materia prelucrării Datelor cu caracter personal, și aprobate la nivelul Spitalului.

### 6.4. Raportare și tratare incidente de securitate

1. Incidentul de securitate în domeniul protecţiei datelor cu caracter personal reprezintă orice eveniment, acţiune, inacţiune sau împrejurare de natură să afecteze confidenţialitatea, integritatea sau disponibilitatea acestor date.

2. Incidentele de securitate în legătură cu protecţia datelor cu caracter personal pot fi:
   a. incidente tehnice (electronice);
   b. incidente operaţionale (fizice);
   c. incidente administrative (procedurale).

3. În principal, constituie incident de securitate:
   a. nerespectarea actelor normative privind datele cu caracter personal;
   b. pierderea, sustragerea, înlocuirea, alterarea sau distrugerea neautorizată ori accidentală a datelor cu caracter personal;

c. forţarea accesului, accesul neautorizat sau interzicerea accesului autorizat la datele cu caracter personal;
d. modificarea neautorizată şi nejustificată a datelor cu caracter personal;
e. copierea neautorizată pe suport de date extern sau executarea de fotocopii ale documentelor care conţin date cu caracter personal fără aprobarea şefului structurii care le gestionează;
f. nerespectarea regulilor privind depozitarea, manipularea sau distrugerea mediilor de stocare în uz pe care sunt stocate date cu caracter personal sau a celor care sunt scoase din uz;
g. nerespectarea cerinţelor legale privind primirea şi distribuirea corespondenţei / circuitul documentelor în Instituţie;
h. producerea altor evenimente care afectează confidenţialitatea, integritatea şi disponibilitatea informaţiilor stocate, procesate sau transmise.

4. Soluţionarea incidentelor se realizează de personalul SCJU Cluj-Napoca, cu înştiinţarea Autorităţii Naţionale privind Protecţia Datelor cu Caracter Personal de către Responsabilul cu protecţia datelor cu caracter personal.

5. Investigarea incidentelor se realizează de către o comisie condusă de managerul SCJU Cluj-Napoca şi este compusă din responsabilul cu protecţia datelor cu caracter personal şi şeful nemijlocit al lucrătorului implicat în incident, fiind luate deîndată *măsuri de limitare, cât este posibil, a prejudiciilor apărute în urma producerii incidentelor.*

6. Investigaţia stabileşte:
a. dacă au fost respectate procedurile privind prelucrarea datelor cu caracter personal;
b. dacă au fost prelucrate ilegal datele cu caracter personal;
c. dacă există persoane care au avut acces la datele cu caracter personal la care se referă incidentul de securitate şi stabilirea identităţii acestora şi a motivului/împrejurărilor care au permis accesul acestora la datele cu caracter personal;
d. măsuri preventive, corective sau dacă este cazul măsuri disciplinare.

7. În cazul în care se constată că au fost prelucrate ilegal datele cu caracter personal se aplică prevederile legale în vigoare.

## 7. REGULI „CLEAN DESK”

Pentru a îmbunătăți securitatea și confidențialitatea informațiilor, SCJU Cluj-Napoca a adoptat reguli „Clean Desk” pentru stațiile de lucru, pentru computere și imprimante.

Acest lucru asigură că toate informațiile sensibile și confidențiale, fie că sunt pe hârtie, un dispozitiv de stocare sau un dispozitiv hardware, sunt blocate sau eliminate în mod corespunzător când o stație de lucru nu este utilizată. Aceste reguli vor reduce riscul accesului neautorizat, pierderii și deteriorării informațiilor în timpul și în afara orelor normale de funcționare sau atunci când stațiile de lucru sunt lăsate nesupravegheate. Regulile reprezintă un control important al securității și confidențialității și sunt necesare pentru respectarea GDPR.

Aceaste reguli se aplică întregului personal (permanent, temporar și contractat) care lucrează în cadrul Spitalului.

### 7.1. Reguli

Ori de câte ori un birou nu este ocupat pentru o perioadă lungă de timp, se vor aplica următoarele reguli:

1. toate documentele sensibile și confidențiale trebuie să fie scoase de pe birou și blocate într-un sertar sau dulap de depozitare. Acestea includ dispozitive de stocare în masă, cum ar fi CD-uri, DVD-uri și unități USB.
2. toată hârtia de deșeuri care conține informații sensibile sau confidențiale trebuie plasată în cutii confidențiale dedicate, preferabil ruptă anterior.
3. stațiile de lucru pentru calculatoare trebuie să fie blocate atunci când biroul este neocupat și închis complet la sfârșitul zilei de lucru.
4. laptopurile, tabletele și alte dispozitive hardware trebuie să fie scoase de pe birou și blocate într-un sertar sau dulap de depozitare.
5. cheile pentru accesarea sertarelor sau a dulapurilor de depozitare nu trebuie lăsate nesupravegheate la un birou.
6. imprimantele și faxurile trebuie tratate cu aceeași atenție, respectiv:
    a. orice lucrare de imprimare care conține documente sensibile și confidențiale trebuie recuperată imediat. Când este posibil, ar trebui să se utilizeze funcția "Imprimare blocată".
    b. toate documentele rămase la sfârșitul zilei de lucru vor fi eliminate corespunzător.

### 7.2. Conformitate

Această politică va fi monitorizată oficial de către DPO - ul numit la nivelul Spitalului și poate include inspecții aleatorii și planificate.

### 7.3. Neconformitate

Orice angajat sau contractant, față de care s-a constatat faptul că a încălcat aceste reguli, poate face obiectul unor măsuri disciplinare, până la încetarea contractului de muncă.

## 8. REGULI „BRING YOUR OWN DEVICE" (BYOD)

Spitalul **acordă** angajaților dreptul de a utiliza smartphone-uri personale la locul de muncă, însă nu au voie să acceseze rețeaua Spitalului de pe acestea. Spitalul își rezervă dreptul de a revoca acest privilegiu, dacă utilizatorii nu respectă politicile și procedurile impuse.

Spitalul **acordă** angajaților dreptul de a utiliza laptop-uri personale la locul de muncă acolo unde nu există astfel de resurse la nivel de secție/compartiment/laborator/serviciu/birou. Spitalul își rezervă dreptul de a revoca acest privilegiu dacă utilizatorii nu respectă politicile și procedurile impuse sau dacă Spitalul pune la dispoziția secției /compartimentului/laboratorului /serviciului/biroului dispozitivul propriu.

Aceste reguli au rolul de a proteja securitatea și integritatea infrastructurii de date și tehnologii a Spitalului. Excepții limitate de la aceste reguli pot apărea prin prisma variațiilor de dispozitive și de platforme.

Angajații trebuie să accepte termenii și condițiile stabilite în această politică pentru a putea conecta dispozitivele lor la rețeaua SCJU Cluj-Napoca.

### 8.1. Utilizare acceptabilă

Operatorul definește utilizarea acceptabilă, ca fiind acele activități care susțin direct sau indirect activitatea Spitalului. SCJU Cluj-Napoca definește folosirea personală acceptabilă în timpul programului de lucru ca o comunicare personală rezonabilă și limitată, cum ar fi citirea.

Angajații nu sunt blocați de la accesarea anumitor site-uri în timpul orelor de lucru / în timp ce sunt conectați cu laptopul personal la rețeaua Spitalului, la discreția sa. Spitalul își rezervă dreptul de a interzice angajaților accesarea anumitor site-uri dacă în viitor apreciază că este necesar.

Dispozitivele nu pot fi utilizate în niciun moment pentru:

- stocarea sau transmiterea unor materiale ilicite;
- stocarea sau transmiterea unor informații privind proprietatea intelectuală aparținând altor instituții;
- acțiuni de hărțuire a altor persoane;

Următoarele aplicații sunt permise: cum ar fi vremea, aplicațiile de productivitate, etc.

Angajații pot utiliza dispozitivul mobil personal pentru a accesa următoarele resurse deținute de Spital: e-mail, calendare, contracte, documente. **Nu au voie, însă, să acceseze baza de date medicale a SCJU Cluj-Napoca.**

### 8.2. Dispozitive și suport

Sunt permise laptopurile personale, având sistemul de operare Windows sau mac OS X.

Problemele de conectivitate sunt soluționate de Biroul Informatică; angajații ar trebui să contacteze producătorul dispozitivului pentru probleme legate de sistemul de operare sau hardware.

Dispozitivele trebuie să fie prezentate la Biroul Informatică pentru asigurarea corespunzătoare a locurilor de muncă și configurarea aplicațiilor standard, cum ar fi browserele, software-ul de productivitate a biroului și instrumentele de securitate, înainte de a putea accesa rețeaua.

### 8.3. Securitate

Pentru a preveni accesul neautorizat, dispozitivele trebuie să fie protejate prin parolă utilizând caracteristicile dispozitivului și este necesară o parolă puternică pentru a accesa rețeaua Spitalului.

Politica Spitalului privind setarea unei parole puternice este: parolele trebuie să aibă cel puțin cinci caractere din care o literă mare, una mică și un simbol. Parolele vor fi schimbate la fiecare 120 de zile.

Dispozitivul trebuie să se blocheze cu o parolă sau un cod PIN dacă este inactiv timp de cinci minute.

După cinci încercări de conectare eșuate, dispozitivul se va bloca. Se va contacta Biroul informatică pentru a se redobândi accesul.

Este strict interzisă accesarea rețelelor rădăcină care oferă posibilitatea de a instala aplicații, teme sau diferite fișiere care, în principiu, nu sunt autorizate, ba chiar interzise pe sistemul de operare, cum ar fi root (Android) sau jailbreake (iOS).

Angajații sunt în mod automat împiedicați să descarce, să instaleze și să utilizeze orice aplicație care nu apare în lista de aplicații aprobate de Spital.

Laptopurile personale care nu se află în lista de dispozitive acceptate ale Spitalului nu au voie să se conecteze la rețea.

Smartphone-urile aparținând angajaților, care sunt numai pentru uz personal, nu au voie să se conecteze la rețea.

Accesul angajaților la datele Spitalului este limitat pe baza profilurilor utilizatorilor definite de Biroul informatica și aplicate automat.

### 8.4. Riscuri. Disclaimere

În timp ce Biroul informatică va lua toate măsurile de precauție pentru a preveni pierderea datelor personale ale angajatului, în cazul în care trebuie să șteargă de la distanță un dispozitiv, este responsabilitatea angajatului de a lua măsuri de precauție suplimentare, cum ar fi copierea de rezervă a e-mail-urilor, a contactelor, a documentelor etc.

Spitalul își rezervă dreptul de a deconecta dispozitivele sau de a dezactiva serviciile fără notificare.

Dispozitivele pierdute sau furate trebuie să fie raportate SCJU Cluj-Napoca în termen de 24 de ore. Angajații sunt responsabili pentru notificarea imediată după pierderea unui dispozitiv. Angajații trebuie să-și folosească dispozitivele în mod etic în orice moment și să respecte politica de utilizare acceptabilă a Spitalului.

Angajații sunt responsabili personal pentru toate costurile asociate cu dispozitivul său. Angajatul își asumă răspunderea deplină pentru riscuri, inclusiv, dar fără a se limita la, pierderea parțială sau completă a datelor Spitalului și a datelor personale din cauza unei erori de sistem de operare, erori, viruși, malware și/sau alte defecțiuni software/ hardware sau programare, erori care fac dispozitivul inutilizabil.

SCJU Cluj-Napoca își rezervă dreptul de a lua măsuri disciplinare corespunzătoare până la încetarea contractului individual de muncă, pentru nerespectarea acestor reguli.

## 9. SUPRAVEGHERE VIDEO

Pentru protejarea securității pacienților și a oricăror alți vizitatori, cât și pentru asigurarea pazei și protecției bunurilor acestora, ale Operatorului și/sau ale angajaților acestuia, clădirile și curțile Operatorului sunt protejate prin supraveghere video/înregistrarea imaginilor obținute prin mijloace de supraveghere video.

Pentru aceste scopuri, persoanele vizate, anterior menționate, precum și bunurile utilizate de acestea când sosesc la, accesează sau vizitează clădirile Operatorului și/sau spațiile exterioare adiacente, sunt filmate cu mijloace de supraveghere video, instalate în locuri vizibile și utilizate în conformitate cu reglementările legale în vigoare.

Supravegherea video are loc doar în spațiile destinate publicului, inclusiv pe căile de acces situate în interiorul sau exteriorul clădirilor Operatorului, locul amplasării mijloacelor de supraveghere video fiind semnalat prin intermediul unei pictograme care conține o imagine reprezentativă și are vizibilitate suficientă.

Imaginile înregistrate prin utilizarea mijloacelor de supraveghere video vor fi transmise de către Operator către organele de poliție și alte autorități cu atribuții privind apărarea drepturilor și libertăților fundamentale ale persoanei, a proprietății private și publice, prevenirea, descoperirea și sancționarea infracțiunilor, respectarea ordinii și liniștii publice, în condițiile legii. Imaginile astfel obținute nu vor fi transmise în străinătate.

Informarea persoanelor vizate cu privire la prelucrarea Datelor Personale prin mijloace de supraveghere video are loc într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun,

în format electronic. La solicitarea persoanei vizate, informaţiile pot fi furnizate verbal, cu condiţia ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

Un sistem de supraveghere video era deja funcțional în cadrul Spitalului Clinic Județean de Urgență Cluj-Napoca înainte de aplicarea Regulamentului (UE) 679/2016 și de emiterea Legii nr. 129 din 15 iunie 2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Procedurile, totuși, au fost revizuite de atunci pentru a se conforma recomandărilor stabilite în Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului 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 în Legea nr. 102 din 3 mai 2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal - Republicare*).

O revizuire periodică va fi întreprinsă la doi ani de către compartimentele responsabile cu asigurarea securității și va analiza: necesitatea menținerii în uz a sistemului; îndeplinirea scopului declarat; posibile alternative adecvate la sistem; dacă prezenta politică respectă în continuare Legea nr. 102 din 3 mai 2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal - Republicare*) și Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului 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).

Sistemul de supraveghere prin mijloace video, cuprinde:

- Clădirea Direcțiune, Cluj-Napoca, str. Clinicilor nr. 3-5;
- Clădirea Ginecologie I, Cluj-Napoca, str. Clinicilor nr. 3-5;
- Clădirea Medicală I – secțiile: Medicină internă, Cardiologie și Gastroenterologie, str. Clinicilor nr. 3-5;
- Clădirea UPU, Cluj-Napoca, str. Clinicilor nr. 3-5;
- Clădirea Chirurgie I, Cluj-Napoca, str. Clinicilor nr. 3-5;
- Clădirea Oftamologie, Cluj-Napoca, str. Clinicilor nr. 3-5;
- Curtea SCJU Cluj-Napoca, str. Clinicilor nr. 3-5;
- Clădirea Palat Nou, (Medicală II) str. Clinicilor nr. 2-4;
- Clădirea Diabet Nutriție și Boli Metabolice, Cluj-Napoca, str. Clinicilor nr. 2-4;
- Clădirea Ginecologie II – Stanca, Cluj-Napoca, str. Bulevardul 21 Decembrie 1989 nr. 57;
- Secțiile Ortopedie I și II, str. Traian Moșoiu, nr.47;
- Compartiment Clinic Chirurgie Orală și Maxilo-Facială, Cluj-Napoca, Calea Moților nr. 33;
- Secția Clinică Chirurgie Orală și Maxilo-Facială, Cluj-Napoca, Strada Cardinal Iuliu Hossu 37;
- Complexul Neurologie, Cluj-Napoca, Strada Victor Babeș, nr. 43:
    - Pavilion 3;

- Pavilion 4;
- Pavilion 5;
- Pavilion 6;

- Institut IMOGEN, Cluj-Napoca, (în curtea Complexului Neurologie).

Amplasarea camerelor a fost atent revizuită pentru a asigura limitarea pe cât posibil a monitorizării zonelor care nu prezintă interes pentru scopul urmărit.

Dispozitivul de înregistrare este amplasat într-un spațiu protejat (birou administrativ – sistemul care deservește curtea Clinicilor 3-5; cabină personal pază (portar) – Palat Nou; birou asistente șefe, secretariate sau alte încăperi cu acces restricționat pentru sistemele din secții clinice/compartimente, secretariatul secției/compartimenului unde este instalat sistemul), neexistând posibilitatea sustragerii suportului de stocare sau a dispozitivului, în special în timpul producerii unui eveniment.

Nu sunt monitorizate zonele în care există un nivel ridicat al așteptărilor privind viața privată, precum birourile, toaletele și alte locații similare.

Se supraveghează prin mijloace video:

-zonele de acces și spațiile destinate publicului de pe holurile Spitalului (în general căi de acces, holuri, scări, parcări ale clădirilor);

-împrejurimile clădirilor, pentru a proteja spațiile exterioare (curțile clădirilor).

Sistemul de supraveghere video nu este utilizat în alt scop decât cel notificat. În circumstanțe excepționale imaginile pot fi transferate organelor de cercetare, în cadrul unei investigații disciplinare sau penale.

Sistemul video al SCJU Cluj-Napoca nu are ca scop captarea (de ex. prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (de ex. indexare, creare de profiluri) care dezvăluie "categorii speciale de date", iar instituția nu intenționează să utilizeze sistemul de supraveghere și în mod ad-hoc, respectiv cu caracter temporar, de circumstanță.

Sistemul de supraveghere video este un sistem static. Are ca funcţie înregistrarea imaginilor şi este echipat cu senzori de mişcare. Sistemul poate înregistra orice mişcare detectată de camerele instalate în zona supravegheată, alături de dată, oră şi locaţie. Toate camerele sunt funcţionale 24 de ore, 7 zile pe săptămână.

Sistemul poate fi accesat din exterior, prin intermediul internetului, dacă este cunoscută adresa de IP static al DVR-ului, precum și userul și parola. Pentru accesarea DVR ului de pe smartphone este necesar un program compatibil cu DVR-ul, precum și cunoașterea userului și a parolei.

Atunci când este necesar, calitatea imaginilor permite recunoaşterea celor care trec prin zona de acţiune a camerelor. Pentru o mai mare siguranţă a prelucrării datelor care pot fi obţinute în urma supravegherii video, camerele sunt fixe (fără funcţie de zoom), astfel utilizatorul nu poate modifica perimetrul/ scopul supravegherii. Sistemul este utilizat de către personalul de pază de la punctul de control doar pentru supraveghere, acesta nu are dreptul de operare a sistemului sau de a consulta înregistrările sistemului, doar vizualizează în timp real ecranul calculatorul cu imaginile de pe camere.

Nu există interconexiune cu alte sisteme și nu se înregistrează sunetul.

Accesul este strict limitat la angajații autorizați, în birourile unde se află sistemul de supraveghere video.

Pentru a proteja securitatea sistemului video şi pentru a spori gradul de protecţie a vieţii, au fost introduse următoarele măsuri tehnice şi organizatorice:

- limitarea timpului de stocare a materialului filmat, în conformitate cu cerinţele de securitate;

- toţi utilizatorii cu drept de acces au semnat Acorduri de confidenţialitate, prin care se obligă să respecte prevederile legale în domeniu;

- dreptul de acces se acordă utilizatorilor pe baza nevoii de a cunoaşte, doar pentru acele resurse care sunt strict necesare pentru îndeplinirea atribuţiilor de serviciu;

- doar administratorii de sistem, numiți în acest sens de către Spital, au dreptul de a accesa fișierele înregistrate în sistem, la cererea conducerii unității;

- administratorii de sistem vor fi consultați înainte de achiziţionarea sau instalarea oricărui nou sistem video de protecţie.

Accesul la imaginile stocate și/sau la arhitectura tehnică a sistemului de supraveghere video este limitat la un număr redus de persoane, ce au conturi limitate, și este determinat prin atribuţiile specificate în fișa postului (în ce scop şi ce tip de acces):

- Managerul Spitalului, care este desemnat ca persoană responsabilă de managementul și protecția datelor obținute prin sistemul de supraveghere video, calitate ce o deține pe perioada exercitării funcției;

- responsabilul cu protecția datelor;

-firma de specialitate care derulează mentenanța sistemului, în caz de nevoie, la solicitare.

**SCJU Cluj-Napoca impune limite în privința persoanelor care au dreptul:**

**- să vizioneze materialul filmat în timp real** – imaginile care se derulează în timp real sunt accesibile personalului de pază care efectuează serviciul la Postul de pază (pentru sistemul care deservește clădirea Medicală II);

- șeful serviciului administrativ, șeful biroului administrativ și personalul administrativ din biroul unde este montat calculatorul și monitorul pentru sistemul de supraveghere care deservește curtea Clinicilor 3-5;

- personalul desemnat de către șefii de secții clinice/compartimente pentru sistemele care deservesc secțiile/compartimentele respective (de regulă asistentele șefe sau personalul din secretariat);

**-să vizioneze înregistrarea materialului filmat** – vizionarea prin derulare a imaginilor înregistrate se face în cazuri temeinic justificate, cum ar fi cazurile prevăzute de lege și incidentele de securitate, de către responsabilul cu protecția datelor și managerul Spitalului. De asemenea, au acces la imaginile stocate: - șeful Serviciului administrativ; șeful Biroului administrativ și economist 1A, pentru sistemul de supraveghere care deservește curtea Clinicilor 3-5;

- personalul desemnat de către șefii de secții clinice/compartimente pentru sistemele care deservesc secțiile/compartimentele respective;

- personalul societăților care asigură mentenanța sistemelor conform obligațiilor contractuale.

**- să copieze, să descarce, șă șteargă sau să modifice orice material filmat** – doar persoanele special desemnate;

Administratorii sistemului semnează o declaraţie de confidenţialitate.

SCJU Cluj-Napoca are obligația punerii la dispoziția organelor judiciare (poliție, parchet, instanță de judecată) la solicitarea scrisă a acestora, și cu aprobarea conducerii Spitalului, înregistrările video în care este surprinsă săvârșirea unor fapte de încălcare a legii.

Orice activitate de dezvăluire a datelor personale către terţi va fi documentată şi supusă unei analize riguroase, privind pe de-o parte necesitatea comunicării, şi pe de altă parte

compatibilitatea dintre scopul în care se face comunicarea şi scopul în care aceste date au fost colectate iniţial pentru prelucrare (de securitate şi control acces). În aceste cazuri, va fi consultat Responsabilul cu protecția datelor și managerul Spitalului. Orice situaţie de dezvăluire va fi consemnată de administratorul sistemului în Registrul de evenimente al sistemului.

Astfel, poate fi permis accesul unor terțe persoane pentru vizualizarea înregistrărilor, în cazul în care persoana respectivă a fost prejudiciată în vreun fel în raza de acțiune a sistemului de supraveghere, dar numai pentru locul și intervalul orar în care a survenit situația semnalată, și numai cu acordul conducerii Spitalului.

În cazuri excepționale, dar cu respectarea garanțiilor descrise mai sus, se poate acorda acces Comisiei Disciplinare, în cadrul unei anchete disciplinare, cu condiția ca informațiile să ajute la investigarea unei infracțiuni sau a unei abateri disciplinare de natură să prejudicieze drepturile și libertățile unei persoane.

Sistemul de supraveghere video nu este utilizat pentru verificarea prezenţei la program sau evaluarea performanţei la locul de muncă.

Orice încălcare a securităţii în ceea ce priveşte camerele video este indicată în Registrul de evenimente al sistemului.

Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video este proporțională cu scopul pentru care se prelucrează datele, astfel că imaginile sunt stocate pentru o perioadă de 30 (treizeci) de zile, în funcție de capacitatea de stocare, după care se șterg automat (se suprascriu) în ordinea în care au fost înregistrate.

În cazul producerii unui incident de securitate, durata de păstrare a materialului filmat relevant poate depăși limitele normale, în funcție de timpul necesar investigării suplimentare a incidentului de securitate.

Păstrarea este documentată riguros, iar necesitatea păstrării este revizuită periodic.

SCJU Cluj-Napoca garantează că asigură respectarea drepturilor ce revin persoanelor vizate, conform legii. Toate persoanele implicate în activitatea de supraveghere video și cele responsabile de administrarea imaginilor filmate, vor respecta procedura operațională privind asigurarea securității datelor cu caracter personal în vigoare.

Informarea primară a persoanelor vizate se realizează în mod clar și permanent, prin intermediul unui semn adecvat, cu vizibilitate suficientă și localizat în zona supravegheată, astfel încât să semnalizeze existența camerelor de supraveghere, dar și pentru a comunica informațiile esențiale privind prelucrarea datelor personale (afișe).

Persoanele vizate sunt atenționate asupra existenței sistemului de supraveghere video și a proprietarului, prin note informative corespunzătoare, care cuprind scopul prelucrării și identifică SCJU Cluj-Napoca ca operator al datelor colectate prin intermediul supravegherii video.

De asemenea, pe site-ul SCJU Cluj-Napoca (https://scjucluj.ro/) va fi publicată prezenta politică, pentru persoanele care doresc să obțină mai multe informații legate de activitatea de supraveghere video desfășurată la nivelul instituției.

Persoana desemnată ca responsabil cu protecția datelor captate prin sistemul de supraveghere video va asigura actualizarea informărilor, corespunzător realităților existente în cadrul activităților desfășurate de Spital.

Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc, deţinute de Spital, de a solicita intervenţia (ştergere/actualizare/rectificare/anonimizare) sau de a se opune prelucărilor, conform legii. Orice cerere de a accesa, rectifica, bloca şi/sau şterge date cu caracter personal ca urmare a utilizării

camerelor video, ar trebui să fie adresată Spitalului, iar o copie a acesteia trebuie trimisă către Responsabilul cu protecția datelor.

În cazul în care persoana vizată are alte întrebări privind prelucrarea de către Spital a datelor personale care o privesc, se poate adresa conducerii spitalului, departamentului juridic sau responsabilului cu protecția datelor personale.

Răspunsul la solicitarea de acces, intervenţie sau opoziţie se dă în termen de 30 zile calendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amânare a răspunsului, de asemenea i se va comunica şi procedura care va urma pentru soluţionarea cererii.

Dacă există solicitarea expresă a persoanei vizate, se poate acorda dreptul de a vizualiza imaginile înregistrate care o privesc sau i se poate trimite o copie a acestora. Imaginile furnizate vor fi clare, în măsura posibilităţii, cu condiţia de a nu prejudicia drepturile terţilor (persoana vizată va putea vizualiza doar propria imagine, imaginile altor persoanelor care pot apărea în înregistrare vor fi editate astfel încât să nu fie posibilă recunoaşterea/identificarea lor).

În cazul unei asemenea solicitări, persoana vizată este obligată să se identifice dincolo de orice suspiciune (să prezinte actul de identitate când participă la vizionare), să menţioneze data, ora, locaţia şi împrejurările în care a fost înregistrată de camerele de supraveghere. De asemenea, persoana vizată va prezenta şi o fotografie recentă astfel încât utilizatorii desemnaţi, să o poată identifica mai ușor în imaginile filmate.

Există posibilitatea refuzării dreptului de acces, în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune şi în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu dacă în imagini apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

Spitalul Clinic Județean de Urgență Cluj-Napoca își rezervă dreptul de a completa, modifica, revizui prezenta politică de supraveghere video ori de câte ori consideră că este necesar. Anexa 1 face parte integrantă din prezenta politică și reprezintă informarea persoanelor vizate cu privire la faptul că obiectivul este supravegheat video.

## 10. SECURITATEA ACTIVITĂȚILOR

SCJU Cluj-Napoca aplică măsurile tehnice şi organizatorice adecvate pentru protejarea datelor împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei rețele, precum şi împotriva oricărei alte forme de prelucrare ilegală.

Aceste măsuri asigură un nivel de securitate adecvat în ceea ce privește riscurile pe care le reprezintă prelucrarea, precum și în ceea ce privește natura datelor care trebuiesc protejate.

- Sunt documentate deciziile care se iau în privinţa necesităţii prelucrării datelor cu caracter personal pentru îndeplinirea sarcinii în interes public sau exerciţiul autorităţii;
- Este identificată în legislaţia aplicabilă, sarcina relevantă sau autoritatea cu care se acţionează;
- Se includ în nota de informare aspecte referitoare la scopuri sau baza legală de prelucrare a datelor cu caracter personal.
- Fiecare structură va completa un Registru de lucru în care sunt menţionate datele cu caracter personal care au fost prelucrate.

Incidentul în domeniul protecției datelor, stocate sau transmise, reprezintă orice eveniment care afectează confidențialitatea, integritatea sau disponibilitatea acestor date.

În principal, constituie incident privind protecția datelor:

- pierderea, sustragerea, înlocuirea, alterarea sau distrugerea neautorizata ori accidentală a datelor;
- modificarea neautorizată şi nejustificată a datelor;
- accesul neautorizat la mediile pe care sunt stocate date.

Reprezintă risc de incident următoarele:

- nerespectarea regulilor privind depozitarea, utilizarea sau distrugerea mediilor de stocare în uz pe care sunt păstrate date;
- orice situație de natură să afecteze confidențialitatea, integritatea sau disponibilitatea datelor.

Orice incident de protecția datelor trebuie comunicat în cel mai scurt timp responsabilului cu protecția datelor, în vederea notificării ANSPDCP despre acest fapt sau a operatorului de date în cazurile în care SCJU Cluj-Napoca acționează ca Împuternicit.

Notificarea către ANSPDCP trebuie formulată în termen de 72 h de la momentul la care Operatorul a luat la cunoștință despre incident.

Securitatea fizică se asigură prin desfășurarea neîntreruptă a unor activități/acțiuni efectuate în scopul asigurării unui nivel de securitate adecvat specificului activității fiecărui obiectiv al spitalului, cât și pentru adaptarea permanentă la condițiile de mediu în care își desfășoară societatea activitatea:

1. Documentele ce conţin date cu caracter personal, adresate Instituţiei de reprezentanţi ai persoanelor juridice sau persoane fizice, se vor înregistra la Secretariatul SCJU Cluj-Napoca;
2. Circulaţia documentelor ce conţin date cu caracter personal în cadrul Instituţiei se va face conform procedurii elaborate de şeful fiecărei structuri şi aprobată de conducerea spitalului;
3. Toate structurile din cadrul SCJU Cluj-Napoca vor înregistra şi vor ţine evidenţa tuturor documentelor ce conţin date cu caracter personal intrate, a celor întocmite pentru uz intern, precum şi a celor ieşite, potrivit legii;
4. În toate birourile angajaţilor din cadrul SCJU Cluj-Napoca se vor păstra documentele ce conţin date cu caracter personal în condiţii corespunzătoare, asigurându-le împotriva accesului neautorizat, distrugerii, degradării, sustragerii ori difuzării în alte condiţii decât cele prevăzute de lege;
5. În scopul asigurării păstrării documentelor ce conţin date cu caracter personal, pe durată determinată, în scopuri legale, acestea se îndosariază şi se arhivează la sfârşitul fiecărui an calendaristic, conform Nomenclatorului arhivistic aprobat la nivelul Instituţiei, în baza Legii Arhivelor Naţionale;
6. Documentele ce conţin date cu caracter personal aflate în încăperile instituţiei vor fi depozitate în fişete prevăzute cu încuietori, inclusiv în timpul programului, pe birou fiind numai documentul/dosarul la care se lucrează în momentul în care ocupantul biroului se găseşte în încăpere;
7. În situaţia în care o încăpere nu va fi deajuns pentru desfăşurarea activităţii profesionale de către angajaţi şi totodată pentru depozitarea documentelor care stau la baza activităţii respective, se vor căuta soluţii pentru prevenirea eventualelor incidente privind protecţia datelor cu caracter personal:

> o încăpere mai mare în care să fie loc deajuns pentru angajaţi şi pentru documente sau

> încă o încăpere, în care să fie depozitate documentele lângă cea în care-şi desfăşoară activitatea angajaţii ori

> analizarea activităţii ce se desfăşoară în fiecare încăpere şi redistribuirea spaţiilor de lucru componentelor structurale din cadrul SCJU Cluj-Napoca, astfel încât să fie asigurată protecţia documentelor letrice şi a celor de pe computere;

8. Angajaţii SCJU Cluj-Napoca nu trebuie să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane referitor la datele cu caracter personal;
9. Fiecare copiator va avea câte un Registru în care vor fi scrise documentele ce conţin date cu caracter personal de pe care s-au făcut copii, în câte exemplare, când (data şi ora), motivul, de către cine şi semnătura celui care a efectuat copiile;
10. Activitatea ce include supravegherea prin sistemul video instalat în spital se va desfăşura în conformitate cu procedura de lucru în acest sens, întocmită de personalul tehnic;
11. Va fi ţinută evidenţa tuturor staţiilor de lucru IT din instituţie şi vor fi întocmite proceduri de lucru de către persoana desemnată de conducerea instituţiei;
12. Computerele trebuie să aibă instalate programe antivirus actualizate şi configurarea eficientă a firewall-ului;
13. Niciun computer nu va avea acces la orice aplicaţie ci numai la cea/cele de care este nevoie în vederea îndeplinirii atribuţiilor de serviciu;
14. Unităţilor de lucru IT&C pe care sunt prelucrate date cu caracter personal le va fi restricţionat accesul la reţeaua internet, rămânând validă numai conectarea pentru update şi folosirea adresei de e-mail de pe domeniul SCJU Cluj-Napoca.
15. Niciun computer nu va conţine alte date cu caracter personal decât cele pentru care este autorizat utilizatorul;
16. Niciun utilizator nu va folosit tehnica IT&C, proprietatea instituţiei, în interes propriu;
17. Niciun utilizator al computerelor SCJU Cluj-Napoca nu va accesa adresa de e-mail personală, creată pe un alt domeniu, utilizând computerul instituţiei;
18. Pentru asigurarea confidenţialităţii datelor şi informaţiilor procesate şi stocate pe echipamentele IT&C din dotare, precum şi pentru protecţia şi securitatea reţelei informatice, se impune accesarea acestora prin identificarea şi autentificarea utilizatorilor;
19. Identificarea şi autentificarea în sistem se realizează prin introducerea unui cod de identificare atribuit de către administratorul de sistem al SCJU Cluj-Napoca, însoţit de introducerea unei parole, aceasta putând fi schimbată de utilizator;
20. Utilizatorii răspund pentru securitatea parolelor şi a conturilor personale;
21. Codurile de identificare şi parolele sunt unice, personale şi netransmisibile. Se interzice folosirea lor în comun, de către mai mulţi utilizatori chiar dacă aceeaşi staţie IT este folosită, pe rând de mai mulţi angajaţi;
22. Documentele care conţin coduri de identificare şi parole de acces vor fi arhivate numai dacă acestea nu se mai află în uz;
23. La părăsirea staţiei de lucru este obligatorie deconectarea utilizatorului sau blocarea calculatorului pe contul de utilizator conectat. Deblocarea staţiei se va putea face doar de către utilizatorul conectat sau administratorul de sistem, în caz de necesitate;
24. În cazul unei situaţii de modificare a competenţelor sau raporturilor de serviciu, administratorul de sistem al SCJU Cluj-Napoca ia măsuri de revocare / suspendare a drepturilor de acces, astfel încât prelucrarea datelor cu caracter personal să se facă numai de către personalul autorizat şi numai în exercitarea atribuţiilor de serviciu ale acestora;
25. Acordarea de permisiuni suplimentare, restrângerea permisiunilor sau dezactivarea conturilor se face în baza solicitărilor scrise, în care se va menţiona motivul acordării/restrângerii permisiunilor sau dezactivării contului utilizatorului respectiv. Personalul care asigură

funcţionarea computerelor şi reţelei IT&C va răspunde în scris despre realizarea cerinţelor. Toate aceste documente se vor anexa la Fişa echipamentului;
26. Utilizatorii nu trebuie să încerce să acceseze informaţii, programe sau aparatura IT&C a SCJU Cluj-Napoca pentru care nu au autorizaţie sau consimţământ explicit;
27. Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor ce conţin date cu caracter personal prelucrate de SCJU Cluj-Napoca;
28. Utilizatorii nu trebuie să divulge sau să înstrăineze nume de conturi, parole şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare;
29. Utilizatorii nu trebuie să facă copii neautorizate şi/sau să distribuie fără consimţământul persoanei vizate, documente ce conţin date cu caracter personal;
30. Conturile de utilizator care nu au fost folosite mai mult de 90 de zile vor fi dezactivate;
31. Tipurile de acces şi operaţiunile permise utilizatorului, strict necesare pentru îndeplinirea atribuţiilor de serviciu, se stabilesc conform atribuţiilor din Fişa postului fiecărui utilizator;
32. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul SCJU Cluj-Napoca, orice incident de securitate celui ce se ocupă de administrarea reţelei;
33. Nici un utilizator al computerelor SCJU Cluj-Napoca nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a staţiei/staţiilor de lucru la care a avut acces. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu SCJU Cluj-Napoca;
34. Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi asigurată. Pentru aceste situaţii, confidenţialitatea şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale ale SCJU Cluj-Napoca se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora;
35. Memoria externă autorizată, pe care se salvează informaţii ce conţin date cu caracter personal, va fi depozitată într-un spaţiu adecvat, sub controlul administratorului de reţea ce asigură buna funcţionare a aparaturii IT din instituţie;
36. Nu este permisă scoaterea din instituţie a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD), decât cu aprobare prealabilă din partea conducerii instituţiei.
37. Instalarea oricărui produs software este interzis a se efectua de către personal neautorizat;
38. Este interzisă instalarea oricărui produs software care ar putea periclita securitatea reţelei, cât şi introducerea de către utilizatorii din cadrul SCJU Cluj-Napoca a unor programe răuvoitoare în reţea;
39. Utilizarea aplicaţiilor informatice se face numai în conformitate cu procedurile, normele de lucru şi metodologiile de exploatare, întocmite de administratorul de sistem şi utilizatorii computerelor, aprobate;
40. Accesarea informaţiilor stocate în bazele de date se realizează numai în interesul îndeplinirii atribuţiilor profesionale, iar furnizarea acestor informaţii este permisă numai în conformitate cu prevederile legale;
41. Imprimarea datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru această operaţiune. Utilizatorii sunt obligaţi să respecte procedurile interne specifice, precum şi Politica de securitate;

42. Administratorul de sistem care asigură întreţinerea funcţionării aparaturii IT&C va şterge de pe orice staţie de lucru, proprietatea SCJU Cluj-Napoca, orice program sau fişier care nu are legătură cu scopul muncii respective. Exemple de astfel de programe sau fişiere, dar nu limitate la: jocuri, programe de comunicare a mesajelor (AOL, Yahoo Messenger, MSN etc.), fişiere cu muzică (mp3, wav etc.), fişiere grafice (bmp, gif, jpg etc.), programe tip freeware şi shareware;
43. Uşa fiecărui birou se încuie la sfârşitul programului de ultima persoană care iese din încăpere, cheile fiind depuse în fişetul de la intrarea în clădire, în grija celui ce asigură serviciul de pază;
44. Descărcarea paginii web de documentele care conţin semnături şi ştampile şi înlocuirea cu documente de pe care au fost şterse semnăturile şi ştampilele, astfel încât persoanelor fizice angajate ale instituţiei să nu le fie utilizate în mod ilegal datele cu caracter personal expuse;
Perimetrul şi holurile interioare al instituţiei sunt supravegheate video şi în caz de alarmă intervin imediat angajaţii, aceştia sesizând evenimentul Poliţiei Locale, atunci când situaţia o impune.

## 11. PERSOANE ÎMPUTERNICITE DE OPERATOR

În anumite condiții expres reglementate, datele cu caracter personal pot fi prelucrate de către SCJU Cluj-Napoca, prin intermediul unor Persoane împuternicite.Vor putea avea acces la datele cu caracter personal furnizorii de servicii cum ar fi, dar fără a se limita la, furnizorii de servicii și sisteme IT, diverși partenerii contractuali (exemplu: companiile specializate în furnizarea serviciilor de pază, care asigură supravegherea video la nivelul Spitalului, furnizorii de servicii de mentenanță a aparaturii etc.), avocați, contabili, auditori sau alți profesioniști care au obligația păstrării secretului profesional. În vederea asigurării serviciilor medicale complete, datele pacienților vor fi furnizate medicilor colaboratori ori clinicilor și laboratoarelor partenere, cu care există încheiate acorduri de confidențialitate.

Împuterniciții sunt obligați să respecte cerințele Operatorului pentru siguranța prelucrării și să ia măsurile tehnice și organizatorice necesare pentru asigurarea protecției Datelor cu caracter personal.

Datele transmise Destinatarilor vor fi adecvate, pertinente și neexcesive prin raportare la scopurile în care au fost colectate.

## 12. ATRIBUȚII ȘI RESPONSABILITĂȚI

1. Structurile şi persoanele responsabile pentru asigurarea protecţiei datelor cu caracter personal, prelucrate de către SCJU Cluj-Napoca, sunt:

**a.** SCJU Cluj-Napoca, în calitate de coordonator al Politicii de securitate a obiectivului care contribuie la:

- stabilirea măsurilor de securitate fizice şi video pentru toate clădirile în care-şi desfăşoară activitatea;
- elaborarea şi actualizarea politicii de securitate a obiectivului şi a procedurilor în domeniu.
- Incheierea unui act aditional la contractul de munca sau includerea unei clauze in contractul de munca, in care sa fie prevazuta **obligatia de confidentialitate a acestora in raport cu datele personale prelucrate.** Desi aceasta obligatie poate reiesi din cele standard prevazute de Codul Muncii, cu siguranta ca o detaliere care sa faca trimitere expresa la datele cu caracter personal, nu poate avea decat un impact pozitiv asupra angajatorului;
- coordonarea activităţii personalului care asigură accesul şi supravegherea video la toate clădirile în care-şi desfăşoară activitatea;

- asigurarea accesului la datele înregistrate de sistemul tehnic de securitate cu aprobarea SCJU Cluj-Napoca;
- monitorizarea activităţii, instruirea şi evaluarea periodică a utilizatorilor în ceea ce priveşte cunoaşterea, respectarea şi aplicarea prevederilor politicii de securitate şi a procedurilor.
- soluţionarea incidentelor de securitate în scopul minimizării efectului negativ al acestora.
- protecţia fizică a documentelor ce conţin date cu caracter personal care se găsesc în Instituţie;
- controlul accesului persoanelor care intră/ies în/din cladirile Instituţiei;

**b.** Utilizatorii - personalul desemnat din cadrul SCJU Cluj-Napoca - care sunt obligaţi:

- să cunoască şi să respecte prevederile Regulamentului (UE) 679/2016, ale Legii 190/2018 şi ale celorlalte acte normative privind prelucrarea datelor cu caracter personal;
- să informeze persoana vizată, atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condiţiile legii, cu privire la: identitatea operatorului, scopul in care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute si consecinţele refuzului de a le pune la dispoziţie, drepturile prevăzute de Regulamentul (UE) 679/2016, condiţiile in care pot fi exercitate aceste drepturi, respectiv să ofere orice alte informaţii a căror furnizare este impusă prin dispoziţii ale Autorităţii Naţionale, ţinând seama de specificul prelucrării;
- să prelucreze numai datele cu caracter personal solicitate sau strict necesare îndeplinirii atribuţiilor de serviciu si să acorde sprijin Responsabilului cu protecţia datelor cu caracter personal pentru realizarea activităţilor specifice ale acestuia/acesteia;
- să cunoască şi să respecte prevederile procedurilor privind prelucrarea datelor cu caracter personal şi cele privind securitatea sistemului informatic cu care intră în contact;
- să respecte măsurile de securitate şi regulile stabilite prin procedurile interne;
- să informeze de îndată conducerea SCJU Cluj-Napoca şi Responsabilul cu protecţia datelor cu caracter personal despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situaţie in care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoştinţă;
- să răspundă direct de securitatea şi conţinutul informaţiilor, de aparatura IT&C încredinţată;
- să se asigure că informaţiile în posesia cărora intră sunt transmise numai persoanelor autorizate;
- să întreţină corespunzător aparatura din componenţa sistemului informatic (menţinerea curăţeniei suprafeţelor exterioare, evitarea şocurilor mecanice, etc.);
- să anunţe pe administratorul de sistem când se observă posibile probleme/breşe în sistemul de securitate şi acces al Instituţiei, întrebuinţare greşită sau încălcare a regulamentelor în vigoare sau funcţionare anormală a echipamentelor IT;

Totodată, utilizatorilor le este interzisă mutarea tehnicii IT (cu excepţia celor mobile), repoziţionarea cablurilor de reţea sau de alimentare, instalarea sau dezinstalarea echipamentelor periferice. Aceste operaţiuni se realizează prin solicitare scrisă şi numai de către administratorul de sistem al SCJU Cluj-Napoca.

Fiecare structură implicată are obligaţia de a actualiza fişele posturilor personalului din subordine cu atribuţii în domeniul protecţiei datelor cu caracter personal, când situaţia o impune.

## 13. MĂSURI PREVENTIVE

Angajații înțeleg pericolul reprezentat de atacurile cibernetice sau cele de tip social (social engineering), precum și repercusiunile pe care aceste atacuri le pot avea asupra Operatorului, asupra angajaților acestuia sau a persoanelor vizate.

Pentru a se asigura un standard ridicat de securitate, Operatorul organizează instruiri cu privire la vulnerabilitățile datelor personale și măsurile preventive de securitate ce se adoptă în cazul atacurilor cibernetice.

Angajatul va fi informat cu privire la atacurile precum:

- **Phishing**: prin care atacatorii utilizează e-mail-urile de tip spam pentru a direcționa victimele către site-uri web create de atacatori astfel încât datele personale să fie introduse pe acel site web;
- **Social engineering**: manipularea rău-intenționată a anumitor persoane prin care angajații sunt convinși să disemineze date cu caracter confidențial;
- **DNS poisoning**: Otrăvirea cache este un atac în care datele corupte sunt inserate în baza de date cache a serverului de nume DNS (Domain Name System). Atacatorul intenționează să trimită răspunsuri duplicate de la un DNS impostor pentru a redirecționa un nume de domeniu la o nouă adresă IP. Noua adresă IP este cel mai probabil controlată de atacator și este utilizată pentru a răspândi viermii de calculator și alte programe malware.

*SCJU Cluj-Napoca își rezervă dreptul de a completa, modifica, revizui prezenta politică de confidențialitate ori de câte ori consideră că este necesar.*

**APROBAT,**
**MANAGER**
**Prof.Dr. Gherman Claudia**

Responsabil cu protecția datelor
Danciu Dorel

## Cuprins: