



ISO 9001

LL-C (Certification)

**CONSILIUL JUDEȚEAN BRAȘOV
SPITALUL CLINIC DE OBSTETRICĂ GINECOLOGIE**

„DR. IOAN AUREL SBÂRCEA“

B R A Ș O V, 500025, Str. G.Barițiu Nr.36

C.U.I. 4443183

E-mail : secretariat@maternitatea.ro

Tel. 0368 202012

Fax: 0368 202055

Operator de date cu caracter personal nr.15158

Nr. 3777 / 24.05.2018



**REGULAMENT INTERN AL SCOG "DR.I.A.SBARCEA" BRASOV IN CONFORMITATE
CU REGULAMENTUL NR 679/27.04.2016 PRIVIND PROTECTIA DATELOR**

• **OBIECT-OBIECTIV**

Prezentul regulament stabileste normele referitoare la protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal ,precum si normele referitoare la libera circulatie a datelor cu caracter personal.

• **DOMENIUL DE APLICARE**

Prezentul regulament se aplica prelucrării datelor cu caracter personal , efectuata total sau partial prin mijloace automatizate precum si prelucrării prin alte mijloace decat cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenta a datelor.

SCOG "DR.I.A.SBARCEA" inregistrat in registrul de evidenta a prelucrarilor de date cu caracter personal nr .15158 , prin intermediul Compartimentului Statistica prelucreaza datele pacientilor cu caracter personal: codul numeric personal,seria si numarul actului de identitate , date privind starea de sanatate s.a. , prin mijloace automatizate /manual avand ca scop "servicii de sanatate".

Totodata SCOG prelucreaza datele cu caracter personal ivite in legatura cu aparitia raporturilor de munca /serviciu ale angajatiilor , prin Biroul RUNOS.

- **DEFINITII**

- *Date cu caracter personal = inseamna orice informatii privind o persoana fizica identificata sau identificabila(o persoana vizata); o persoana identificabila este o persoana care poate fi identificata ,direct sau indirect, in special prin referire la un element de identificare , date de localizare, un identificator online, sau la unul sau mai multe elemente specifice , proprii identitatii sale fizice, fiziologice ,genetice, psihice,economice, cultural sau sociale;*
- *Prelucrare= inseamna orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra datelor cu caracter personal, cu sau fara utilizarea de mijloace automatizate;*
- *Date privind sanatatea=inseamna date cu caracter personal legate de sanatatea fizica sau mental a unei persoane fizice, inclusive prestarea de servicii de asistenta medicala , care dezvaluie informatii despre starea de sanatate a acesteia;*

- **ORGANIZAREA MASURILOR DE PROTECTIE A DATELOR MEDICALE CU CARACTER PERSONAL**

- *Documentatia medicala , inclusiv fisele medicale ale pacientilor inregistrati in cadrul spitalului , inclusiv alte formulare si registre care contin date cu caracter personal si medical se considera purtatoare de date cu caracter personal.*
- *Aceasta documentatie urmeaza a fi pastrata de angajatii institutiei in birouri si spatii special destinate(arhiva , statistica, birouri medici si asistente medicale, laboratoare)*
- *Fisele medicale dupa externarea pacientilor sunt pastrate in arhiva spitalului in conformitate cu cerintele nomenclatorului arhivistic /legislatia in vigoare*
- *Transmiterea fiselor medicale in alte sectii se asigura numai prin personalul medical si auxiliar medical responsabil*
- *Nu se permite eliberare a fiselor medicale in original pacientilor(reprezentantilor acestora s.a)*
- *In scopul evitarii divulgarii datelor cu caracter personal si medical se cere obligatoriu stabilirea identitatii persoanei care receptioneaza fisele medicale prin verificarea actului de identitate /legitimatiei de serviciu /etc*
- *Nu se permit discutii prin telefon referitor la datele cu caracter personal si medical*

- **CONSINTAMANTUL LA PRELUCRAREA DATELOR CU CARACTER PERSONAL SI MEDICAL**

Datele personale ale pacientilor sunt prelucrate (preluate, prelucrate, stocate) de catre SCOG, in conformitate cu prevederile Regulamentului UE 679/2016 si actele normative in vigoare din domeniul sanatatii, in scopul efectuării de servicii medicale.

- **SECURITATEA DATELOR CU CARACTER PERSONAL SI MEDICAL DE CATRE ANGAJATII SCOG**

- *Sefii de sectie/compartimente organizeaza masuri de instruire a persoanelor din subordine privind protectia datelor cu caracter personal avand ca referinta prevederile prezentului Regulament*
- *Totii salariatii SCOG efectueaza prelucrarea datelor cu caracter personal conform atributiilor functionale*
- *Nu se admite prelucrarea datelor cu caracter personal in alte scopuri decat in scopul exercitarii obligatiunilor functionale*
- *Nu se admite divulgarea datelor medicale cu caracter personal , persoanelor terte prin telefon sau prin comunicare directa fara stabilirea identitatii persoanei si a termenului legal al solicitarii*
- *Nu se admite divulgarea datelor medicale cu caracter personal in discutii intre salariatii , cu exceptia cazurilor de necesitate de serviciu*
- *Personalul medical este obligat sa explice pacientilor , solicitantilor motivele nedivulgarii datelor medicale cu caracter personal ,sau refuzul eliberarii unor documente medicale ,etc.*
- *Computerele , serverele , alte terminale de acces sunt amplasate in locuri cu acces limitat pentru persoane straine*
- *Sefii de servicii , personalul medical la locul de munca trebuie sa organizeze plasarea obiectivelor ce contin date cu caracter personal in asa mod ca sa raspunda necesitatii asigurarii securitatii acestora contra accesului nesanctionat, furturilor , incendiilor , inundatiilor si altor posibile riscuri.*

**SECURITATEA DATELOR CU CARACTER PERSONAL/MEDICAL ,
PRELUCRAREA ACESTORA IN MOD MANUAL(PE SUPT DE HARTIE IN
CADRUL SCOG**

- *Fisele medicale din cadrul spitalului (FOGG, formulare ,registre) se considera purtatoare de date cu caracter personal*
- *FOGG a tuturor pacientilor inregistrati in cadrul SCOG sunt pastrate pana la arhivare in cadrul Compartimentului Statistica*

- *Nu se permite discutii la telefon referitor la date cu caracter personal, cu excepția situațiilor când este cunoscută identitatea persoanei*
- *Acordarea asistenței medicale prevede prelucrarea datelor cu caracter personal*
- *Datele cu caracter personal a beneficiarilor de servicii prestate în SCOG sunt prelucrate în scopul efectuării de servicii medicale.*
- *Refuzul pacientului privind furnizarea datelor cu caracter personal nu va afecta calitatea îngrijirilor și tratamentul de care beneficiază în cadrul SCOG, în situația în care prelucrarea este necesară pentru prevenirea unui pericol iminent..*
- *Informațiile înregistrate cu privire la datele cu caracter personal ale pacienților sunt destinate utilizării de către operator și sunt comunicate numai următorilor destinatari:*
 - *MINISTERUL SANITĂȚII, DIRECTIA DE SANITATE BRASOV, CASA DE ASIGURARI DE SANITATE BRASOV, S.N.S.P.M.S*
 - *Organe competente (instanțe judecătorești,) organe de cercetare (Parchet , Poliție)*
 - *Mass – media , numai cu acordul pacientului cu respectarea Legii nr 46/2003 a drepturilor pacientului și a prezentului Regulament*
- *SISTEMUL INFORMATIONAL DE PRELUCRARE A DATELOR CU CARACTER PERSONAL DIN CADRUL SCOG*
 - *Datele cu caracter personal ce se prelucrează sunt următoarele:*
 - *Nume, Prenume*
 - *Data și locul nașterii*
 - *CNP*
 - *Sexul*
 - *Adresa , domiciliu , reședință*
 - *Date privind sănătatea*
 - *Sistemul informational de prelucrare a datelor cu caracter personal din cadrul SCOG este alcătuit din următoarele elemente (mijloace tehnice și soft)*
 - *Stație de lucru*
 - *Servere*

- *Toti utilizatorii (inclusiv personalul care asigura sustinerea tehnica, administratorul de retea , programatori, administratori ai bazelor de date) au un indentificator personal(ID-ul utilizatorului). Pentru confirmarea ID-ului utilizatorului sunt utilizate parole irepetabile de nu mai putin de 7-8 caractere ce contin litere din ambele registre ,cifre si alte semne simbolice.*

❖ *Administrarea identicatorilor utilizatorilor include:*

- *identificarea univoca(irepetitiva) al fiecarui utilizator*
- *verificarea autenticitatii fiecarui utilizator*
- *garantarea factorului ca ID-ul utilizatorului este eliberat unei persoane determinate complet*
- *dezactivarea contului de utilizator dupa o perioada inactiva stabilita in timp*

❖ *Reguli de asigurare a securitatii informationale*

Regulile de asigurare a securitatii informationale in cazul alegerii si folosirii parolei include:

- *Pastrarea confidentialitatii parolelor*
- *Interzicerea inscrierii parolelor pe suport de hartie ,in cazul in care nu se asigura securitatea pastrarii acestora*
- *Modificarea paaarolelor de fiecare data cand sunt prezente indiciile eventualei compromiteri a sistemului sau parolei*
- *Alegerea parolelor calitative cu o marime de minim 7-8 simboluri , care nu contin simboluriidentice consecutive si nu sunt compuse integraldin grupul de cifre sau litere*
- *Este asigurata posibilitatea utilizatorilor de a alege si schimba parolele individuale*
- *Este asigutara blocarea accesului dupa 3 tentativegresite si autentificate*
- *Inainte de acordarea accesului in sistem , utilizatorii sunt informati despre faptul ca folosirea sistemelor informationale de date cu caracter personal este controlata si ca utilizarea neautorizata a acestora se urmareste in conformitate cu legislatia*
- *Totodata se asigura protectia contra infiltrarii programelor daunatoare in softuri destinate prelucrarii datelor cu caracter personal,masura ce asigura posibilitatea reinnoirii automate si la timp a mijloacelor de asigurare a protectiei contra programelor daunatoare si a virusilor*

- *Controalele de securitate a informatiilor de date cu caracter personal se efectueaza cu regularitate cel putin o data pe an .*
- **REGULI CU PRIVIRE LA PROTECTIA DATELOR CU CARACTER PERSONAL IN CADRUL BIROULUI RUNOS-SCOG**
 - *Aceste reguli se refera la stabilirea masurilor telefonice si organizatorice necesare pentru asigurarea sanatatii , confidentialitatii si integritatii datelor cu caracter personal in cadrul RUNOS sunt: orice informatie referitoare la angajati , reflectata in sistemul informational, in dosarul personal , fisa personala ,contractul individual de munca , acte aditionale la CIM , diverse registre specifice biroului Runos*
 - *Colectarea si prelucrarea datelor personale ale salariatului poate fi efectuata exclusiv in scopul angajarii, instruirii , avansarii in serviciu , atestarii , perfectionarii , furnizarii datelor catre: Colegiul Medicilor,ITM, Casa de PENSII, Directia de Sanatate si Asistenta Medicala Brasov, Consiliul Judetan Brasov, Ministerul Sanatatii, Directia de Sanatate Publica;*
 - *Biroul Runos este obligat sa utilizeze datele cu caracter personal ale salariatilor numai in limitele competentelor functionale doar in timpul orelor de program.*
 - *Biroul Runos are obligatia sa excluda sau sa rectifice la solicitarea salariatului datele personale incorecte sau incomplete si a informatiilor care se pastreaza nelegitim*
 - *Biroul Runos nu are dreptul sa obtina si sa prelucreze date referitoare la convingerile politice, religioase , la viata privata.*
 - *Biroul Runos nu are dreptul sa obtina si sa prelucreze date privind apartenenta salariatului la sindicate , asociatii religioase , partide si alte organizatii social politice*
 - *Biroul Runos nu trebuie sa comunice unor terti datele personale ale salariatilor fara acordul scris al acestuia cu exceptia cazurilor prevazute de lege si respectand ierarhizarea de subordonare a SCOG (M.S, D.S.P.,D.S.A.M., C.J. Bv , C.A.S Bv, Finante, Pensii , I.T.M. Ordinul asistentelor, colegiul Medicilor etc)*
 - *Biroul Runos trebuie/ poate sa permita accesul la datele personale ale salariatului doar persoanelor imputernicite necesare exercitarii unor atributii de serviciu(manager, director medical, director financiar contabil, sindicat si altora in conformitate cu legislatia in vigoare)*

- *Biroul Runos are obligatia sa previna persoanele , care in exercitiul functiunii solicita si primesc date cu caracter personal ale salariatilor ca poarta raspundere in conformitate cu legislatia pentru divulgarea lor , luandu-se in considerare prejudiciul adus prin acestea salariatului .*
- *De comun acord cu serviciul IT, Biroul Runos, trebuie sa asigure protectia datelor cu caracter personal in procesul exploatarei sistemului informational , prevenirea scurgerii informatiei , distrugerii , modificarii , copierii.*
- *Nu se admite in cadrul Biroului Runos accesul neautorizat la datele cu caracter personal ale salariatilor , a persoanelor straine*
- *Predarea datelor cu caracter personal de catre Biroul Runos in arhiva institutiei se face conform nomenclatorului arhivistic aprobat.*

• **SECURITATEA BIROULUI RUNOS:**

- *Dulapurile cu dosarele salariatilor permanent inchise*
- *La finele zilei de munca se incuie usile si ferestrele*
- *Nu se admite accesul persoanelor straine la computer*
- *Respectarea cerintelor si asigurarea securitatii contra incendiilor si altor posibile riscuri*

Salariatul are dreptul privind asigurarea protectiei datelor sale personale care se pastreaza in cadrul Biroului Runos:

- *De a primi informatia deplina despre datele sale personale si modul de prelucrare a acestora*
- *De a avea acces liber si gratuit la datele sale personale , inclusiv dreptul la o copie de pe orice act juridic care contine datele personale*
- *De a cere excluderea sau rectificarea datelor personale incorecte sau incomplete , a informatiilor care se pastreaza nelegitim*
- *De a ataca in instanta de judecata orice actiune sau inactiune ilegala a angajatorului admise la obtinerea, pastrarea , prelucrarea si protectia datelor personale ale salariatului.*
- *Personalul Biroului Runos si alte persoane care in exercitiul functiunii au luat cunostinta de datele cu caracter personal , poarta raspundere in conformitate cu legislatia in vigoare , pentru divulgarea acestor date , lundu-se in considerare prejudiciul adus de acestea subiectului de date.*

REGULAMENTUL PRIVIND ASIGURAREA SECURITATII DATELOR CU CARACTER PERSONAL AL PACIENTULUI IN CADRUL SCOG

Regulamentul are scopul de a asigura nivelul corespunzător al protecției datelor cu caracter personal ale persoanelor ce beneficiază de servicii medicale prin aplicarea corespunzătoare a legislației în vigoare cu privire la protecția datelor.

Scopul prelucrării datelor cu caracter personal în cadrul SCOG este prestarea serviciilor medicale acordate pacienților . toate fișele din ambulator , camera de gardă, a pacienților internate pe secțiile SCOG , inclusiv alte formulare și registre , fișe pe suport de hârtie , note la cazurile de deces, certificate extrase, trimiteri la investigații , care conțin date cu caracter personal-se consideră purtătoare de date cu caracter personal.

Întru realizarea scopului de prestare a serviciilor medicale , medicii și asistentele medicale din SCOG dunt în drept de a solicita de la persoana ce se adresează pentru acordarea asistenței medicale la SCOG următoarele date:

- *Numele , prenumele*
- *Data și locul nașterii*
- *Cardul de sănătate*
- *Numărul de telefon*
- *Adresa de domiciliu*
- *Profesia și/sau locul de muncă*
- *CNP*
- *Semnatura*
- *Cetățenia*

Întru respectarea confidențialității datelor cu caracter personal, personalul medical va respecta cu strictețe următoarele reguli:

- *Toate documentele medicale ce conțin date cu caracter medical și personal urmează a fi păstrate în locuri special destinate în dulapuri care se încuie*
- *Nu se admite divulgarea datelor cu caracter personal în discuții între salariați cu excepția cazurilor de necesitate de serviciu*
- *Acordarea asistenței medicale este inițiată la etapa de programare a pacientului și prevede prelucrarea datelor cu caracter personal*
- *Datele cu caracter personal a persoanelor ce beneficiază de servicii medicale în cadrul SCOG sunt prelucrate (preluate, prelucrate, stocate), în conformitate cu prevederile Regulamentului UE 679/2016 și actele normative în vigoare din domeniul sănătății, în scopul efectuării de servicii medicale.*

În conformitate cu Regulamentul UE nr.679/2016 și/sau după caz Legea nr.677/2001, persoana vizată își poate exercita drepturile de acces, de intervenție și de opoziție.

REGULAMENT PRIVIND SUPRAVEGHEREA

PRIN MIJLOACE VIDEO IN CADRUL SPITALULUI CLINIC DE OBSTETRICA-GINECOLOGIE "DR.I.A.SBARCEA"BRASOV

1.

Dispoziții generale

În contextul actual securitatea obiectivelor nu poate fi asigurată fără o supraveghere video eficientă, care să permită, atât monitorizarea în timp real a evenimentelor și persoanelor suspecte, cât și înregistrarea imaginilor video.

Totodată utilizarea unui astfel de sistem include anumite responsabilități și garanții din partea proprietarului de sistem, referitor la prelucrarea și protecția datelor cu caracter personal ce se înregistrează în sistem.

Din acest motiv este necesară stabilirea unui regulament de securitate privind supravegherea prin mijloace video și prelucrarea datelor cu caracter personal preluate și înregistrate în sistemul de monitorizare prin înregistrare video.

2.

Regulamentul privind supravegherea prin mijloace video în cadrul SCOG "Dr.I.A.Sbarcea"Brasov are ca scop:

☐

Stabilirea unui set unitar de reguli care reglementează implementarea și utilizarea sistemului de supraveghere video, în scopul asigurării securității persoanelor și bunurilor, pazei și protecției bunurilor, imobilelor, valorilor și a materialelor cu regim special, respectînd în același timp obligațiile ce revin entității, în calitate de operator de date, conform legislației în vigoare și măsurile de securitate adoptate pentru protecția datelor cu caracter personal, protejarea vieții private, a intereselor legitime și garantarea drepturilor fundamentale ale persoanelor vizate.

☐

Stabilirea responsabilităților privind administrarea și exploatarea sistemului de supraveghere prin mijloace video, precum și cele privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.

☐

Scopul utilizării sistemului video este de a asigura buna administrare și funcționare

a entității, în special în vederea controlului de securitate și pază. De asemenea, sistemul video este necesar pentru a sprijini politicile de securitate instituite de actele normative care reglementează protecția datelor cu caracter personal și contribuie la îndeplinirea atribuțiilor structurii de securitate.

☐

Prezentul Regulamentul descrie măsurile care necesită a fi luate de către SCOG pentru a proteja datele cu caracter personal care sînt prelucrate prin metoda supravegherii video, vieții private și alte drepturi fundamentale și interese legitime ale subiecților.

3.

Zonele supravegheate

☐

Camerele de supraveghere video sînt amplasate în locuri vizibile. Orice utilizare ascunsă a acestora este strict interzisă, cu excepția cazurilor expres reglementate de legislație.

☐

Camerele de supraveghere video sînt amplasate conform anexei nr. 1 al prezentului Regulament.

☐

Nu sînt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum birourile de serviciu și toaletele.

4.

Datele cu caracter personal colectate prin intermediul sistemului de supraveghere video

☐

Sistemul de supraveghere video este dotat cu detector de mișcare. Toate camerele funcționează în regim 24/24 ore și sînt fixate.

☐

La darea în exploatare a sistemului de supraveghere video, persoana împuternicită va primi instructajul referitor la setările sistemului de monitorizare video, respectarea regimului de confidențialitate și dreptul de acces la informația prelucrată în sistemul de evidență.

5.

Limitarea scopului

☐

Sistemul de supraveghere video va fi utilizat numai în scopul în care este notificat, fără a se urmări în special obținerea unor informații pentru anchetele interne sau procedurile disciplinare, cu excepția situațiilor în care se produce un incident de securitate sau se observă un comportament infracțional (în circumstanțe excepționale imaginile pot fi transmise organelor competente în cadrul unor investigații disciplinare sau penale).

☐

În vederea protejării vieții private a altor subiecți decât cei vizați nemijlocit, sistemul video este dotat cu mecanisme care prevăd estomparea imaginii (în caz de necesitate) pentru a face ca întreaga imagine sau o parte a ei, după caz, să fie anonimată.

☐

Persoana responsabilă va gestiona accesul la sistemul de supraveghere video numai cu acordul scris al conducerii SCOG.

6.

Categorii speciale de date cu caracter personal

☐

Sistemul de monitorizare video al SCOG nu are ca scop captarea (spre exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (spre exemplu indexare, creare de profiluri) care constituie categoria specială de date cu caracter personal.

7.

Accesul la datele cu caracter personal și dezvăluirea acestora

☐

Accesul la imaginile video înregistrate în timp real este limitat la un număr redus de angajați ai SCOG care pot fi identificați individual, în conformitate cu lista aprobată de către conducerea entității.

☐

Accesul la imaginile video și/ sau la arhiva în care sînt stocate imaginile înregistrate este permis numai persoanei responsabile din cadrul SCOG.

8.

Protecția sistemului informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video

În vederea securizării sistemului informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video, se aplică următoarele măsuri tehnice și organizatorice:

☐

sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video se păstrează în camera special amenajată;

☐

accesul fizic la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video are numai persoana responsabilă desemnată și conducerea SCOG

☐

accesul la înregistrările video prelucrate este restricționat prin introducerea unui șir de parole;

☐

în cazul deconectării energiei electrice, sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu sursă autonomă de alimentare cu energie electrică (UPS);

☐

sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu firewall care asigură protecția în rețea;

☐

SCOG actualizează în permanență listă persoanelor care au acces la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate)

imaginile video, care descrie în detaliu drepturile de acces ale acestora.

9.

Control Acces

☐

Imaginile captate de sistemul de supraveghere video sînt vizualizate în timp real pe monitoarele din camera de control acces, care reprezintă o încăpere securizată, iar monitoarele nu pot fi văzute din exterior.

☐

Camera de control acces este amplasată în sediul central al entității.

☐

Accesul neautorizat în Camera de control este interzis. Accesul este strict limitat la angajații autorizați: personalul cu funcții de asigurare al securității fizice și

control acces, administratorul de sistem, responsabilii cu securitatea informației și conducerea entității.

☐

De la caz la caz, se poate acorda accesul în Camera de control și altor persoane,

în afara celor menționate mai sus, doar pe bază de autorizare din partea responsabilului de securitate din cadrul entității. Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video, accesul acestora fiind permis strict pentru executarea lucrărilor menționate în autorizarea din partea responsabilului de securitate din cadrul entității.

10.

Pentru a proteja securitatea sistemului video și pentru a spori gradul de protecție a vieții private, au fost introduse următoarele măsuri tehnice și organizatorice:

☐

limitarea timpului de stocare a materialului filmat, în conformitate cu cerințele de securitate și legislația în vigoare privind conservarea datelor.

☐

mediile de stocare (serverele pe care se stochează imaginile înregistrate) se află în spații securizate.

☐

doar administratorii de sistem numiți în acest sens de către operator, și responsabilul de securitate, au dreptul de a accesa fișierele înregistrate în sistem, la cererea conducerii unității.

11.

Drepturi de acces

1.

Accesul la imaginile stocate și/sau la arhitectura tehnică a sistemului de supraveghere video este limitat la un număr redus de persoane și este determinat prin atribuțiile specificate în fișa postului, în care este indicat în ce scop și ce tip de acces este acordat.

2.

SCOG impune limite stricte în privința persoanelor care au dreptul:

☐

să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile responsabililor de securitate și agenților de pază desemnați să desfășoare activitatea de supraveghere;

☐

să vizioneze înregistrarea materialului filmat: vizionarea imaginilor înregistrate se va face în cazuri justificate, cum ar fi cazurile prevăzute expres de lege și incidentele de securitate, de către persoanele special desemnate;

☐

să copieze, să descarce, să șteargă sau să modifice orice material filmat de sistemul de supraveghere video.

3.

Instructaj

☐

Toți membrii personalului cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor.

☐

Această procedură va fi integrată în programul de instruire și îndrumare, pentru toți utilizatorii cu drept de acces și atribuții în operarea sistemului de supraveghere video.

4.

Măsuri de păstrare a confidențialității

12.

Dezvăluirea datelor cu caracter personal

☐

Orice activitate de dezvăluire a datelor personale către terți va fi documentată și supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, și pe de altă parte compatibilitatea dintre scopul în care se face comunicarea și scopul în care aceste date au fost colectate inițial pentru prelucrare.

☐

Orice situație de dezvăluire va fi consemnată de administratorul sistemului într-un Registru de evidență a cazurilor de dezvăluire.

☐

SCOG are obligația punerii la dispoziția organelor judiciare, la solicitarea scrisă a acestora, înregistrările video în care este surprinsă săvârșirea unor fapte de natură contravențională/penală.

☐

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

13.

Durata păstrării înregistrărilor video

☐

Durata păstrării înregistrărilor video este de 30 zile calendaristice, după care acestea se nimicesc automat în ordinea în care au fost înregistrate.

☐

În cazul producerii unui incident de securitate, durata de păstrare a înregistrărilor video poate depăși limitele admisibile de program, în funcție de timpul necesar investigării suplimentare a incidentului de securitate.

14.

Informarea publicului referitor la supravegherea video

Informarea publicului referitor la supravegherea video din cadrul SCOG se efectuează prin pictograme.

☐

SCOG garantează că asigură respectarea drepturilor ce revin persoanelor vizate, în conformitate cu legislația în vigoare. Toate persoanele implicate în activitatea de supraveghere video și cele responsabile de administrarea imaginilor filmate, vor respecta procedurile și regulamentele de acces la date cu caracter personal ale entității.

15.

Informarea persoanelor vizate

☐

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 semnaleze existența camerelor de supraveghere, dar și pentru a comunica informațiile esențiale privind prelucrarea datelor cu caracter personal.

☐

Persoanele vizate sunt atenționate asupra existenței sistemului de supraveghere video și a proprietarului prin note de informare corespunzătoare, care cuprind scopul prelucrării și identifică IMSP "SCMS" ca operator al datelor colectate prin intermediul supravegherii video.

16.

Exercitarea drepturilor de acces, intervenție și opoziție

☐

Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc deținute de SCOG, conform legii.

☐

Orice cerere de a accesa, rectifica, bloca și/sau șterge date cu caracter personal ca urmare a utilizării camerelor video ar trebui să fie adresată direct SCOG.

☐

Răspunsul la solicitarea de acces, intervenție sau opoziție 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 și procedura care va urma pentru soluționarea 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 posibilității, cu condiția de a nu prejudicia drepturile terților (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 recunoașterea/identificarea lor). În cazul unei asemenea solicitări, persoana vizată este obligată:

a.

să se identifice dincolo de orice suspiciune (să prezinte actul de identitate când participă la vizionare), să menționeze data, ora, locația și împrejurările în care a fost înregistrată de camerele de supraveghere.

☐

Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune și în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu dacă în imagini apar și alte persoane și nu există posibilitatea de a obține consimțământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

17.

Auditul securității sistemului de monitorizare video

☐

Auditul securității sistemului de monitorizare video pastrează înregistrări de sistem despre evenimentele produse în activitatea sistemului sau a aplicației, precum și despre activitatea utilizatorului.

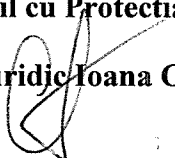
□

În conjuncție cu instrumentele și procedurile respective, auditul securității sistemului de monitorizare video permite promovarea mijloacelor de ajutor pentru a atinge obiective de securitate: evidența acțiunilor utilizatorului, definirea și stabilirea responsabilității individuale, reconstrucția evenimentelor, detectarea intrușilor și problemelor de identificare a evenimentelor.

Intocmit,

Responsabil cu Protecția Datelor

consilier juridic Ioana Cotinghiu



2023.09.27
14:00