Aprobat prin
Hotărârea Consiliului INJ nr.1/7 din 15.01.2020

Modificat prin
Hotărârea Consiliului INJ nr.4/3 din 17.02.2020

REGULAMENTUL
PRIVIND SUPRAVEGHEREA PRIN MIJLOACE VIDEO
ÎN CADRUL INSTITUTULUI NAȚIONAL AL JUSTIȚIEI

1. Dispoziții generale

- Regulamentul privind supravegherea prin mijloace video în cadrul Institutului Național al Justiției (denumit în continuare *Regulament*), stabilește modalitatea de utilizare și funcționare a sistemului de supraveghere prin mijloace video a sediului Institutului Național al Justiției (denumit în continuare *sistem de supraveghere*) și descrie măsurile care necesită a fi luate pentru asigurarea protecției datelor cu caracter personal, care sunt prelucrate prin metoda supravegherii prin mijloace video, vieții private, altor drepturi fundamentale și interese legitime ale subiecților.
- Proprietar al sistemului de supraveghere este Institutul Național al Justiției (denumit în continuare *Institut*), cu statut de persoană juridică, care asigură baza tehnico-materială și instituțională pentru realizarea funcțiilor de post central de dirijare și de gestionare a sistemului, în condițiile legii.
- Organizarea și funcționarea sistemului de supraveghere se efectuează din contul și în limitele mijloacelor aprobate în bugetul de stat și din alte surse prevăzute de legislația în vigoare.
- Mijloacele de supraveghere video se instalează și se utilizează cu respectarea principiului legalității, proporționalității, transparenței și securității.
- Sistemul de supraveghere este utilizat în vederea asigurării bunei administrări și funcționări a entității, securității și pazei acesteia.

2. Regulamentul are drept scop:

- stabilirea unui set unitar de reguli care reglementează implementarea și utilizarea sistemului de supraveghere, în vederea asigurării securității persoanelor, pazei și protecției bunurilor, imobilelor, valorilor și ale materialelor cu regim special, respectând obligațiile ce îi revin entității, în calitate de operator de date, conform Legii nr.133 din 18.07.2011 privind protecția datelor cu caracter personal, precum și măsurile de securitate necesare protecției datelor cu caracter personal;
- protejarea vieții private și a intereselor legitime ale persoanei;
- garantarea drepturilor fundamentale ale subiectului datelor cu caracter personal;
- stabilirea responsabilităților privind administrarea și utilizarea sistemului de supraveghere, întocmirea, avizarea și aprobarea documentelor aferente acestor activități.

3. Zonele supravegheate

- Camerele de supraveghere video sunt amplasate în locuri vizibile, conform anexei nr.1. Orice utilizare ascunsă a acestora este strict interzisă, cu excepția cazurilor expres reglementate de legislație.
- Nu sunt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum ar fi birourile de serviciu, toaletele și alte locații similare.
- Instalarea mijloacelor de supraveghere video se realizează numai în condițiile în care echipamentele sunt orientate exclusiv asupra căilor de acces și perimetrului acestor bunuri, fără ca în raza lor de acoperire să fie vizualizate alte spații publice ori bunurile terților.

4. Datele cu caracter personal colectate prin intermediul sistemului de supraveghere

- Sistemul de supraveghere este dotat cu detectoare de mișcare.

- Toate camerele de supraveghere video sunt fixate și funcționează în regim 24/24 ore, 7 zile pe săptămână.
- La darea în exploatare a sistemului de supraveghere, persoana împuternicită va primi instrucțiunile referitoare la setările acestuia, precum și cu privire la respectarea regimului de confidențialitate și dreptul de acces la informația prelucrată în sistemul de evidență.
- Sistemul de supraveghere nu are ca scop captarea (spre exemplu: prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (spre exemplu: prin indexare sau creare de profiluri), care constituie categorie specială de date cu caracter personal.

5. Limitarea scopului

- Sistemul de supraveghere va fi utilizat numai în scopul în care este notificat, fără a se urmări obținerea unor informații pentru anchete interne sau proceduri 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 de supraveghere 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 anonimizată.
- Șeful Centrului de Informații Juridice va gestiona accesul la sistemul de supraveghere la indicația conducerii Institutului.

6. 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 Institutului, care pot fi identificați individual, în conformitate cu lista aprobată de conducerea Institutului.
- Accesul la imaginile video și/sau la arhiva în care sunt stocate imaginile înregistrate este permis numai persoanei responsabile în conformitate cu Politica de securitate a Institutului și numai cu acordul scris al conducerii.
- Vizualizarea și/sau efectuarea copiilor din fișierele temporare în care sunt stocate imaginile video, este permis numai cu acordul scris al conducerii.
- Solicitarea de către organele de drept ale Republicii Moldova a unor copii din fișierele temporare în care sunt stocate imaginile video se examinează în conformitate cu prevederile Codului de procedură penală, Codului contravențional, ale altor legi și acte normative relevante.

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

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

- sistemul informațional se păstrează în camera special amenajată (conform amplasării indicate în anexa nr.1);
- responsabilul de protecție a datelor cu caracter personal și responsabilii de securitate informațională (Secția tehnologii informaționale) sunt consultați înainte de achiziționarea sau instalarea oricărui sistem de supraveghere nou;
- toate sistemele de supraveghere corespund cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului Republicii Moldova nr.1123 din 14.12.2010;
- acces fizic la sistemul informațional are numai persoana responsabilă desemnată și conducerea Institutului;

- accesul la înregistrările video prelucrate este restricționat prin introducerea de parole;
- în cazul deconectării energiei electrice, sistemul informațional este dotat cu sursă autonomă de alimentare cu energie electrică (UPS);
- sistemul informațional este dotat cu firewall care asigură protecția acestuia în rețea;
- camerele de supraveghere video sunt instalate astfel încât să fie monitorizate video doar acele spații, care sunt identificate în analiza de risc ca având nevoie de protecție suplimentară, utilizatorii sistemului de supraveghere fiind instruiți în acest sens;
- conducerea Institutului actualizează în permanență listă persoanelor care au acces la sistemul informațional, fiind descrise în detaliu drepturile de acces ale acestora.

8. Control Acces

- Imaginile captate de sistemul de supraveghere sunt 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 Institutului.
- Accesul neautorizat în camera de control este interzis.
- Se permite accesul în camera de control acces:
    a) personalului cu funcții de asigurare al securității fizice și control acces,
    b) administratorului sistemului de supraveghere,
    c) personalului responsabil de securitatea informației,
    d) conducerii Institutului,
    e) altor persoane, cu permisiunea și sub supravegherea responsabilului de securitate din cadrul Institutului. Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video, accesul acestora fiind permis strict pentru executarea lucrărilor stabilite.

9. În vederea asigurării securității sistemului de supraveghere și sporirii gradului de protecție al vieții private, sunt 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 și protejate prin măsuri de securitate fizică;
- toți utilizatorii cu drept de acces la sistemul de supraveghere semnează o declarație pe proprie răspundere (conform anexei nr.3), prin care se obligă să respecte prevederile legale în domeniu;
- utilizatorilor sistemului de supraveghere li se acordă drept de acces doar către resursele care sunt strict necesare pentru îndeplinirea atribuțiilor de serviciu;
- doar administratorii sistemului de supraveghere numiți în acest sens de către operator, au dreptul de a accesa fișierele înregistrate în sistemul de supraveghere, la indicația conducerii Institutului.

10. Drepturi de acces

- Accesul la imaginile stocate și/sau la arhitectura tehnică a sistemului de supraveghere 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.
- Conducerea Institutului impune limite stricte în privința persoanelor care au dreptul:
    a) să vizioneze materialul filmat în timp real;
    b) să vizioneze înregistrarea materialului filmat;
    c) să copieze, să descarce, să șteargă sau să modifice orice material filmat de sistemul de supraveghere.
- Toți membrii personalului cu drepturi de acces beneficiază de o instruire inițială în domeniul

protecției datelor cu caracter personal, fiind integrată în programul de instruire și îndrumare a personalului Institutului.

- Șeful Centrului de Informații Juridice asigură ca întregul personal din subordine, implicat în operarea sistemului de supraveghere, să fie instruit și informat cu privire la toate aspectele funcționale, operaționale și administrative ale acestei activități.
- Imediat după instructaj, fiecare participant cu drept de acces la sistemul de supraveghere semnează un acord de confidențialitate.

11. Dezvăluirea datelor cu caracter personal

- Orice activitate de dezvăluire a datelor personale către terți este documentată și supusă unei analize riguroase privind necesitatea comunicării și compatibilitatea dintre scopul în care se face comunicarea și scopul în care aceste date au fost colectate inițial pentru prelucrare.
- Orice situație de dezvăluire este consemnată de administratorul sistemului într-un Registru de evidență a cazurilor de dezvăluire (anexa nr.4).
- Sistemul de supraveghere nu este utilizat pentru verificarea prezenței angajaților Institutului sau pentru evaluarea performanței acestora la locul de muncă.
- În cazuri excepționale, poate fi acordat acces la datele din sistemul de supraveghere altor subdiviziuni ale Institutului, cu condiția ca informațiile să ajute la investigarea unei infracțiuni, accident de muncă sau a unei abateri disciplinare de natură să prejudicieze drepturile și libertățile unei persoane fizice sau juridice.

12. 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 termenul prevăzut mai sus, în funcție de timpul necesar investigării suplimentare a incidentului de securitate.
- Camera de supraveghere video de la punctul de control-acces nr.5 destinat pentru intrarea și ieșirea mijloacelor de transport pe/de pe teritoriul Institutului nu efectuează înregistrări video, dar fotografiază numerele de înmatriculare ale mijloacelor de transport aflate în fața porții, în vederea stabilirii automatizate a dreptului de acces în incinta Institutului.

  [Pct.12 modificat prin Hotărârea Consiliului INJ nr.4/3 din 17.02.2020]

13. Informarea publicului referitor la supravegherea video

- Informarea publicului referitor la supravegherea video din cadrul Institutului se efectuează prin pictograme, conform modelului prevăzut în anexa nr.5.
- Institutul garantează asigurarea respectării drepturilor ce le 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 Institutului care se referă la accesul la datele cu caracter personal.

  [Pct.13 modificat prin Hotărârea Consiliului INJ nr.4/3 din 17.02.2020]

14. 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 și a proprietarului prin note de informare corespunzătoare, care cuprind scopul prelucrării și identifică Institutul ca

operator al datelor colectate prin intermediul supravegherii video.

15. Exercitarea drepturilor de acces, intervenție și opoziție

- Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au drept de acces la datele personale care le privesc, deținute de Institut, de a solicita intervenția asupra lor (ștergere, actualizare, rectificare, anonimizare) sau de a se opune prelucrării acestora, conform legii.
- Orice cerere de a accesa, rectifica, bloca și/sau șterge date cu caracter personal ca urmare a utilizării camerelor de supraveghere video ar trebui să fie adresată conducerii Institutului.
- În cazul în care persoana vizată are alte întrebări privind prelucrarea de către Institut a datelor personale care o privesc, se poate adresa conducerii Institutului.
- Răspunsul la solicitarea de acces, de intervenție sau de opoziție se dă în termen de 15 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 persoane care pot apărea în înregistrare vor fi editate astfel încât să nu fie posibilă recunoașterea/identificarea lor). În cazul unei asemenea solicitări, persoana vizată:
    a) este obligată 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 video;
    b) va prezenta o fotografie recentă astfel încât utilizatorii desemnați să o poată identifica mai ușor în imaginile filmate;
    c) va putea vizualiza doar propria imagine, imaginile persoanelor care pot apărea în înregistrare vor fi editate astfel încât să nu fie posibilă recunoașterea/identificarea lor.
- 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.

16. Auditul securității sistemului de supraveghere

- Auditul securității sistemului de supraveghere (efectuat în corespundere cu Politica de securitate) menține înscrieri 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 supraveghere permite de a promova mijloace 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.
- Auditul securității sistemului de monitorizare video este menit să acorde suport la:
    a) stabilirea consecutivității acțiunilor utilizatorului sau proceselor;
    b) stabilirea când, cine sau ce a stopat funcționarea normală a sistemului;
    c) soluționarea problemei de detectare a intrușilor;
    d) detectarea problemelor de funcționare a sistemului informatic în regim online.