

**Ministerul Educației și Cercetării
al Republicii Moldova**

ORDIN

04.04.2026 nr. 1372

mun. Chișinău

**Cu privire la aprobarea Instrucțiunii privind
instalarea și utilizarea sistemelor de supraveghere video
în instituțiile de educație timpurie**

În conformitate cu prevederile art. 140, alin. (1) lit. z¹) din Codul educației nr. 152/2014 (Monitorul Oficial al Republicii Moldova, 2014, nr. 319-324, art. 634), pct. 9, subpct. 9.10) din Regulamentul privind organizarea și funcționarea Ministerului Educației și Cercetării, aprobat prin Hotărârea Guvernului nr. 146/2021, emit următorul

ORDIN:

1. Se aprobă Instrucțiunea privind instalarea și utilizarea sistemelor de supraveghere video în instituțiile de educație timpurie, conform Anexei la prezentul ordin.
2. Direcția generală politici în învățământul general va informa instituțiile de educație timpurie cu prevederile prezentului ordin.
3. Controlul executării prezentului ordin se atribuie dnei Valentina Olaru, Secretar de Stat.
4. Prezentul Ordin se publică în Monitorul Oficial al Republicii Moldova.

Ministru

Dan PERCIUN

Ex.: A.Prisăcaru, 022-232785

INSTRUCȚIUNE**privind instalarea și utilizarea sistemelor de supraveghere video
în instituțiile de educație timpurie****Capitolul I. Dispoziții generale**

1. Instrucțiunea privind instalarea și utilizarea sistemelor de supraveghere video în instituțiile de educație timpurie (în continuare - Instrucțiune) stabilește cadrul normativ, principiile, condițiile și procedurile privind instalarea, utilizarea, administrarea și controlul sistemelor de supraveghere video în instituțiile de educație timpurie.
2. Sistemele de supraveghere video se instituie exclusiv în vederea asigurării securității copiilor, a personalului și a bunurilor instituției, cu respectarea dreptului la viață privată, a demnității persoanei, a interesului superior al copilului și a legislației privind protecția datelor cu caracter personal. La evaluarea oricărei măsuri de supraveghere video se iau în considerare efectele psihologice potențiale asupra copiilor, în special riscul inhibării exprimării libere, al afectării dezvoltării naturale și al creării unui sentiment de supraveghere permanentă.
3. Prezenta Instrucțiune se aplică tuturor instituțiilor de educație timpurie publice și private din Republica Moldova.
4. Obligațiile care revin operatorilor economici, prestatorilor de servicii, persoanelor împuternicite și altor terți implicați în instalarea, întreținerea, administrarea, accesarea sau stocarea imaginilor se stabilesc, potrivit Capitolului IX, prin contractul încheiat cu instituția și se execută în conformitate cu prezenta Instrucțiune. .
5. Prezenta Instrucțiune este elaborată în conformitate cu:
 - 5.1 Constituția Republicii Moldova;
 - 5.2 Codul educației al Republicii Moldova nr. 152/2014;
 - 5.3 Legea nr. 133/2011 privind protecția datelor cu caracter personal;
 - 5.4 Legea nr. 140/2013 privind protecția specială a copiilor aflați în situație de risc și a copiilor separați de părinți;
 - 5.5 Legea nr. 148/2023 privind accesul la informațiile de interes public;
 - 5.6 Hotărârea Guvernului nr. 1211/2016 cu privire la aprobarea Regulamentului sanitar pentru instituțiile de educație timpurie;
 - 5.7 Ordinul MEC nr. 254/2017 cu privire la aprobarea Regulamentul-tip al instituției de educație timpurie;
 - 5.8 Ordinul MEC nr. 592/2020 cu referire la aprobarea Instrucțiunii cu privire la ocrotirea vieții și sănătății copiilor în instituțiile de educație timpurie;
 - 5.9 Ordinul Centrului Național pentru Protecția Datelor cu Caracter Personal nr. 27/2022 privind aprobarea listei operațiunilor de prelucrare a datelor cu caracter personal pentru care este obligatorie efectuarea evaluării impactului asupra protecției datelor.
6. La aplicarea prezentei Instrucțiuni se țin cont și de recomandările și liniile directoare emise de Centrul Național pentru Protecția Datelor cu Caracter Personal (în continuare-CNPDCP), în măsura în care acestea nu contravin actelor normative prevăzute la pct.5.
7. În sensul prezentei Instrucțiuni, se utilizează următoarele noțiuni:
 - 7.1 Sistem de supraveghere video – ansamblu de echipamente și aplicații utilizate pentru captarea, transmiterea, stocarea și vizualizarea imaginilor video;
 - 7.2 Operator de date – instituția de educație timpurie, reprezentată de director, care stabilește scopurile și mijloacele de prelucrare a datelor prin sistemul de supraveghere video;

- 7.3 Persoană împuternicită – persoana fizică sau juridică ce prelucrează date în numele instituției de educație timpurie;
- 7.4 Persoană vizată – orice persoană fizică identificată sau identificabilă surprinsă de sistemul de supraveghere video;
- 7.5 Evaluarea impactului asupra protecției datelor – procesul de evaluare prealabilă a riscurilor pentru drepturile și libertățile persoanelor vizate, efectuat în condițiile legii;
- 7.6 Secvență relevantă – partea din înregistrare necesară pentru clarificarea unui incident concret.

Capitolul II. Principii și condiții generale

- 8. Prelucrarea imaginilor prin intermediul sistemelor de supraveghere video se realizează cu respectarea următoarelor principii:
 - 8.1 legalitate, echitate și transparență;
 - 8.2 scop determinat, explicit și legitim;
 - 8.3 necesitate și proporționalitate;
 - 8.4 minimizarea datelor;
 - 8.5 limitarea stocării;
 - 8.6 integritate și confidențialitate;
 - 8.7 responsabilitate.
 - 9. Instalarea și utilizarea sistemelor de supraveghere video nu poate fi întemeiată exclusiv pe consimțământul sau acordul persoanelor vizate.
 - 10. Informarea și consultarea părinților sau a reprezentanților legali, a personalului și a altor persoane vizate constituie garanții procedurale și nu substituie temeiul juridic al prelucrării.
 - 11. Sistemul de supraveghere video poate fi instituit numai dacă:
 - 11.1 există un scop legitim și determinat;
 - 11.2 necesitatea măsurii este justificată în scris;
 - 11.3 nu există măsuri alternative mai puțin intruzive care să asigure în mod suficient atingerea scopului urmărit;
 - 11.4 a fost efectuată evaluarea impactului asupra protecției datelor, în cazurile prevăzute de lege;
 - 11.5 sunt instituite măsuri tehnice și organizatorice adecvate pentru protecția datelor.
 - 12. Supravegherea video nu trebuie să aducă atingere nejustificată vieții private, demnității persoanei sau interesului superior al copilului. Se prezumă că supravegherea continuă în spațiile în care copiii își petrec timpul în mod obișnuit este contrară interesului superior al copilului, în absența unui risc specific, grav și documentat.
 - 13. Sistemele de supraveghere video pot fi instalate și utilizate exclusiv pentru:
 - 13.1 protejarea perimetrului și a bunurilor: monitorizarea căilor de acces, a intrărilor/ieșirilor, a perimetrului exterior și a spațiilor tehnice;
 - 13.2 controlul accesului: verificarea persoanelor care intră sau ies din instituție;
 - 13.3 documentarea unui incident specific: înregistrarea unei secvențe relevante în legătură cu un eveniment concret (accident, conflict, faptă cu potențial contravențional sau penal), după producerea acestuia.
- Scopurile enumerate sunt exhaustive și se interpretează restrictiv. Nu constituie scop legitim: monitorizarea curentă a comportamentului copiilor, evaluarea activității personalului sau supravegherea în scop pedagogic.
- 14. Este interzisă utilizarea imaginilor obținute prin sistemele de supraveghere video pentru:
 - 14.1 evaluarea curentă a activității profesionale a personalului;
 - 14.2 monitorizarea pedagogică permanentă a copiilor;
 - 14.3 publicitate, promovare, difuzare publică ori distribuire prin rețele sociale sau aplicații de mesagerie;

14.4 orice alt scop incompatibil cu cele prevăzute la pct.13.

Capitolul III. Clasificarea spațiilor și reguli de amplasare

15. În funcție de nivelul de intruziune, spațiile din cadrul instituției de educație timpurie se clasifică în:

- 15.1 spații standard admisibile;
- 15.2 spații admisibile condiționat;
- 15.3 spații interzise.

16. În categoria spațiilor standard admisibile intră:

- 16.1 căile de acces în instituție, inclusiv intrările și ieșirile;
- 16.2 porțile, perimetrul exterior și alte zone de acces;
- 16.3 coridoarele, holurile și alte spații comune de circulație;
- 16.4 blocul alimentar, depozitele, arhivele, punctele tehnice și alte spații similare.

17. În categoria spațiilor admisibile condiționat intră:

- 17.1 sălile de grupă;
- 17.2 sălile de activitate;
- 17.3 spațiile de joacă interioare și exterioare;
- 17.4 alte spații în care copiii își petrec timpul în mod obișnuit.

18. În categoria spațiilor interzise intră:

- 18.1 dormitoare;
- 18.2 grupurile sanitare, vestiarele, băile și spațiile de igienă;
- 18.3 birourile personale;
- 18.4 cancelaria și spațiile de odihnă ale personalului;
- 18.5 cabinetul medical, spațiul de izolare, spațiile de consiliere sau alte spații în care persoanele au o așteptare ridicată și legitimă de viață privată.

19. Reguli generale de amplasare a camerelor video:

- 19.1 se instalează numai în locuri vizibile;
- 19.2 nu pot fi disimulate, ascunse sau prezentate sub formă de obiecte false;
- 19.3 se poziționează astfel încât să capteze strict zona necesară atingerii scopului declarat;
- 19.4 nu pot fi orientate spre spațiul public exterior sau spre proprietăți învecinate, cu excepția captării incidentale inevitabile.

20. Instalarea camerelor video în spațiile prevăzute la pct. 17 este interzisă ca măsură generală. Prin derogare, aceasta se admite exclusiv în situații excepționale și temporare, pe o perioadă determinată care nu poate depăși 6 luni și numai dacă sunt întrunite cumulativ următoarele condiții:

- 20.1 existența unui risc specific, real și documentat privind securitatea copiilor sau a personalului;
- 20.2 demonstrarea insuficienței altor măsuri mai puțin intruzive;
- 20.3 efectuarea unei evaluări a impactului asupra protecției datelor distincte pentru spațiile respective;
- 20.4 avizul responsabilului cu protecția datelor sau, după caz, al persoanei desemnate;
- 20.5 aprobarea expresă a fondatorului.

La expirarea termenului de 6 luni, continuarea supravegherii necesită o nouă procedură de fundamenteare și o nouă aprobare a fondatorului. Prelungirile succesive sunt permise numai dacă riscul specific și documentat se menține.

Capitolul IV. Procedura de instituire a sistemului

21. Directorul instituției inițiază procedura de instalare a sistemului de supraveghere video numai în baza unui dosar de fundamenteare.

22. Dosarul de fundamentare cuprinde cel puțin:
 - 22.1 nota privind scopul și riscul concret urmărit;
 - 22.2 analiza măsurilor alternative și justificarea insuficienței acestora;
 - 22.3 evaluarea impactului asupra protecției datelor, după caz;
 - 22.4 planul de amplasare a camerelor și descrierea câmpului vizual al fiecărei camere;
 - 22.5 proiectul de semnalizare și de notă informativă;
 - 22.6 termenul de stocare propus și procedura de ștergere;
 - 22.7 lista funcțiilor cu acces la imagini;
 - 22.8 descrierea măsurilor tehnice și organizatorice de securitate;
 - 22.9 proiectul contractului cu eventualii prestatori;
 - 22.10 avizul responsabilului cu protecția datelor sau, după caz, al persoanei desemnate.
23. Instalarea sistemului de supraveghere video se realizează numai după:
 - 23.1 evaluarea necesității și proporționalității măsurii;
 - 23.2 efectuarea evaluării impactului asupra protecției datelor, în cazurile prevăzute de lege;
 - 23.3 consultarea părinților sau a reprezentanților legali și a personalului instituției;
 - 23.4 obținerea avizului responsabilului cu protecția datelor sau, după caz, al persoanei desemnate;
 - 23.5 obținerea aprobării fondatorului.
24. Orice extindere, reconfigurare, schimbare a scopului sau modificare tehnologică semnificativă a sistemului urmează aceeași procedură ca și instituirea inițială.

Capitolul V. Consultarea și informarea persoanelor vizate

25. Consultarea părinților sau a reprezentanților legali se realizează în cadrul unei ședințe organizate de conducerea instituției.
26. În cadrul ședinței prevăzute la pct. 25 se prezintă cel puțin:
 - 26.1 scopul și temeiul instalării sistemului;
 - 26.2 locațiile propuse;
 - 26.3 durata de stocare a imaginilor;
 - 26.4 drepturile persoanelor vizate;
 - 26.5 măsurile de securitate și regulile de acces la imagini.
27. Consultarea are rol de informare și participare a comunității educaționale și nu substituie temeiul juridic al prelucrării.
28. Instituția are obligația de a informa în mod clar, vizibil și accesibil persoanele despre existența sistemului de supraveghere video.
29. Informarea se realizează în două niveluri:
 - 29.1 prin pictograme și informații esențiale afișate vizibil înainte de intrarea în zona supravegheată;
 - 29.2 printr-o notă informativă completă, disponibilă la sediul instituției și, după caz, pe pagina web a acesteia.
30. Nota informativă completă va cuprinde cel puțin:
 - 30.1 scopurile prelucrării;
 - 30.2 zonele supravegheate;
 - 30.3 perioada de stocare;
 - 30.4 destinatarii sau categoriile de destinatari ai imaginilor;
 - 30.5 drepturile persoanelor vizate și modalitatea de exercitare a acestora;
 - 30.6 datele de contact ale responsabilului cu protecția datelor sau ale persoanei desemnate.
31. Informarea se reiterează la începutul fiecărui an de studii și la orice modificare semnificativă a sistemului.

Capitolul VI. Cerințe tehnice și administrarea sistemului

32. Sistemul de supraveghere video trebuie configurat astfel încât să respecte principiul minimizării datelor.
33. Înregistrarea audio este interzisă și se dezactivează implicit.
34. Funcțiile de recunoaștere facială, identificare biometrică, profilare automată sau alte funcții similare sunt interzise.
35. Sistemul trebuie să asigure:
 - 35.1 claritate suficientă a imaginii pentru clarificarea incidentelor;
 - 35.2 indicarea corectă a datei și orei;
 - 35.3 protecția împotriva accesului neautorizat, modificării sau pierderii datelor;
 - 35.4 ștergerea automată a imaginilor la expirarea termenului de retenție.
36. Transmiterea în timp real a imaginilor către părinți, personal sau alte persoane prin aplicații mobile, platforme online, monitoare accesibile publicului sau alte mijloace similare este interzisă.
37. Instituția de educație timpurie, reprezentată de director, are calitatea de operator de date și este responsabilă pentru:
 - 37.1 aprobarea documentelor interne privind funcționarea sistemului;
 - 37.2 asigurarea informării persoanelor vizate;
 - 37.3 desemnarea persoanelor autorizate să acceseze imaginile;
 - 37.4 instruirea personalului relevant;
 - 37.5 monitorizarea respectării regulilor de confidențialitate și securitate;
 - 37.6 gestionarea incidentelor de securitate și, după caz, notificarea autorităților competente.
38. Directorul desemnează, prin act intern, persoana sau persoanele autorizate să administreze sistemul și să acceseze imaginile.
39. Responsabilul cu protecția datelor sau, după caz, persoana desemnată:
 - 39.1 avizează documentele privind sistemul de supraveghere video;
 - 39.2 verifică respectarea regulilor de protecție a datelor;
 - 39.3 ține evidența accesărilor și a extragerilor de imagini;
 - 39.4 monitorizează respectarea termenelor de stocare;
 - 39.5 participă la actualizarea evaluării impactului asupra protecției datelor;
 - 39.6 formulează recomandări de conformare.
40. Monitorizarea în timp real a imaginilor este permisă numai în situații de urgență, alarmă, incident în desfășurare sau risc iminent rezonabil.

Capitolul VII. Accesul la imagini

41. Accesul la imaginile stocate este strict limitat și se acordă numai persoanelor desemnate, în baza atribuțiilor de serviciu și exclusiv în una dintre următoarele situații justificare:
 - 41.1 producerea unui incident care necesită clarificare;
 - 41.2 exercitarea unui drept al persoanei vizate;
 - 41.3 solicitarea legitimă a unui organ de drept sau a unei instanțe;
 - 41.4 audit intern sau verificare de conformitate.
- Orice acces în afara acestor situații este interzis și se consemnează ca incident de securitate.
42. Fiecare acces la imagini și fiecare extragere de secvențe se consemnează într-un registru special.
 43. Imaginile pot fi puse la dispoziția organelor de drept, instanțelor de judecată, autorităților competente sau altor entități abilitate numai în condițiile legii și, după caz, în baza unei solicitări oficiale.

44. Părintele sau reprezentantul legal poate solicita vizualizarea secvenței relevante privind un incident care îl privește direct pe copilul său.
45. Cererea prevăzută la pct.44 se examinează cu respectarea drepturilor și libertăților celorlalte persoane surprinse în imagini și a interesului superior al copilului.
46. Instituția poate satisface solicitarea prin:
- 46.1 vizualizare controlată la sediul instituției;
 - 46.2 punerea la dispoziție a unei secvențe redactate sau blurate, în cazurile permise de lege.
47. Remiterea unei copii a înregistrării se poate efectua în următoarele cazuri:
- 47.1 organelor de drept și instanțelor de judecată, în condițiile legii și în baza unei solicitări oficiale;
 - 47.2 autorităților competente abilitate prin lege să solicite astfel de date.
- Părintele sau reprezentantul legal nu primește o copie a înregistrării, ci poate solicita vizualizarea controlată la sediul instituției a secvenței relevante privind un incident ce îl privește direct pe copilul său, în condițiile pct. 44–46. Remiterea copiei către alți terți este interzisă.
48. Persoana care consideră că supravegherea video sau răspunsul instituției privind accesul la imagini contravine legislației poate sesiza Centrul Național pentru Protecția Datelor cu Caracter Personal.

Capitolul VIII. Stocarea, extragerea și ștergerea imaginilor

49. Imaginile video se păstrează pe perioada strict necesară realizării scopului pentru care au fost colectate, fără a depăși, de regulă, 30 de zile calendaristice.
50. Instituția stabilește, după caz, un termen mai scurt de retenție, dacă acesta este suficient pentru atingerea scopului urmărit.
51. În cazul producerii unui incident, se extrage și se păstrează separat numai secvența relevantă, până la finalizarea procedurilor interne, administrative, contravenționale sau penale, după caz.
52. Extragerea imaginilor se face în baza unui proces-verbal semnat de persoanele implicate.
53. Orice suspendare a ștergerii automate, extragere sau păstrare prelungită a unei secvențe se documentează.
54. Ștergerea imaginilor din fluxul curent se realizează automat și definitiv, prin setările sistemului.
55. Instituția asigură imposibilitatea recuperării neautorizate a imaginilor șterse.

Capitolul IX. Prestatori, control și audit

56. Instalarea, mentenanța, stocarea externă sau alte operațiuni realizate de terți se efectuează numai în baza unui contract scris.
57. Contractul prevăzut la pct.56 include în mod obligatoriu:
- 57.1 obiectul și limitele prelucrării;
 - 57.2 măsurile de securitate aplicabile;
 - 57.3 obligația de confidențialitate;
 - 57.4 interdicția utilizării imaginilor în scop propriu;
 - 57.5 condițiile de acces tehnic la sistem;
 - 57.6 obligațiile privind ștergerea sau returnarea datelor la încetarea raporturilor contractuale.
58. Accesul tehnic al prestatorului la sistem se permite numai cu aprobarea instituției și se consemnează în registrul de acces.
59. Anual, instituția efectuează o revizuire privind:
- 59.1 necesitatea menținerii sistemului;
 - 59.2 proporționalitatea și eficiența măsurii;

59.3 posibilitatea înlocuirii totale sau parțiale cu măsuri mai puțin intruzive;

59.4 respectarea regulilor de protecție a datelor și securitate.

60. În cazul camerelor instalate în spațiile prevăzute la pct.17, revizuirea se efectuează cel puțin o dată la 6 luni.

61. Rezultatele evaluării se consemnează într-un raport intern aprobat de director și transmis fondatorului.

62. Responsabilul cu protecția datelor sau persoana desemnată efectuează anual un audit intern privind funcționarea sistemului și conformitatea acestuia.

63. Raportul de audit va include cel puțin:

63.1 analiza riscurilor;

63.2 incidentele constatate;

63.3 neregulile identificate;

63.4 recomandările de corectare;

63.5 termenul de implementare a măsurilor.

64. Fiecare instituție de educație timpurie aprobă un regulament intern privind supravegherea video, armonizat cu prezenta Instrucțiune.

Capitolul X. Dispoziții finale

65. Se interzice:

65.1 utilizarea imaginilor video în scopuri neautorizate;

65.2 instalarea camerelor ascunse sau a sistemelor false care induc ideea de supraveghere;

65.3 utilizarea sistemului pentru evaluarea curentă a comportamentului copiilor ori a personalului;

65.4 publicarea sau distribuirea imaginilor în afara cadrului legal.

66. Nerespectarea prevederilor prezentei Instrucțiuni atrage răspunderea disciplinară, civilă, contravențională sau penală, după caz, potrivit legii.

67. Până la data intrării în vigoare a Legii nr. 195/2024 privind protecția datelor cu caracter personal, trimiterile din prezenta Instrucțiune la legislația privind protecția datelor se interpretează ca trimiteri la Legea nr. 133/2011 privind protecția datelor cu caracter personal.

68. După intrarea în vigoare a Legii nr. 195/2024, Ministerul Educației și Cercetării va examina necesitatea ajustării prezentei Instrucțiuni.

Anexa nr. 1
la Regulamentul privind instalarea și
utilizarea sistemelor de supraveghere video
în instituțiile de educație timpurie

Model de notă de informare și confirmare de luare la cunoștință

Subsemnatul(a) _____, părinte/reprezentant legal al copilului _____, confirm că am fost informat(ă) de către IET _____ despre instalarea și utilizarea sistemului de supraveghere video în condițiile prevăzute de Instrucțiunea privind instalarea și utilizarea sistemelor de supraveghere video în instituțiile de educație timpurie.

Confirm că am luat cunoștință despre:

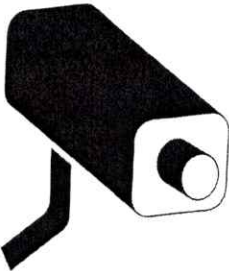
- a) scopurile supravegherii video;
- b) zonele în care sunt instalate camerele;
- c) termenul de stocare a imaginilor;
- d) drepturile persoanelor vizate;
- e) datele de contact ale instituției și ale responsabilului cu protecția datelor.

Data _____

Semnătura _____

Model de pictogramă și informare scurtă

Modelul de pictogramă se elaborează în conformitate cu Formularul tipizat de informare privind efectuarea supravegherii prin mijloace video (pictogramă), aprobat prin Decizia CNPDCP nr. 581 din 10.09.2015, cu modificările ulterioare.

 ATENȚIE! SUPRAVEGHERE VIDEO (/AUDIO*) DURATA: 24/24 TERMENUL DE STOCARE: 	IMAGINILE SUNT ÎNREGISTRATE DE CĂTRE:
	DETALII DE CONTACT OPERATOR:
	DETALII DE CONTACT PERSOANĂ ÎMPUTERNICITĂ*:
	DETALII DE CONTACT PERSOANĂ RESPONSABILĂ CU PROTECȚIA DATELOR*:
	SCOPUL PRELUCRĂRII:
	DREPTURILE SUBIECTULUI DE DATE: subiectul de date cu caracter personal dispune de drepturile prevăzute de Legea nr. 133/2011 privind protecția datelor cu caracter personal. <i>Pentru detalii, accesați informația disponibilă, prezentată de către operator:</i>
	PRIN AFIȘARE LA SEDIU:
	PLASATĂ PE PAGINA WEB:
	*dacă este cazul

Formatul actualizat al pictogramei este disponibil pe pagina web a CNPDCP
(www.datepersonale.md).

Instituțiile utilizează exclusiv formatul aprobat de CNPDCP.

Anexa nr. 3
la Regulamentul privind instalarea și
utilizarea sistemelor de supraveghere video
în instituțiile de educație timpurie

Model de cerere de vizualizare a secvenței relevante

Subsemnatul(a) _____, părinte/reprezentant legal al copilului _____, solicit vizualizarea secvenței video relevante privind incidentul produs la data de _____, în cadrul IET _____.

Descriere succintă a incidentului:

Declar că am luat cunoștință că accesul la imagini se acordă cu respectarea drepturilor celorlalte persoane surprinse în înregistrări și în condițiile legii.

Data _____

Semnătura _____

Anexa nr. 4
la Regulamentul privind instalarea și
utilizarea sistemelor de supraveghere video
în instituțiile de educație timpurie

Model de registru de acces la imagini

Nr.	Data și ora accesului	Numele și funcția persoanei	Temeiul/ scopul accesului	Intervalul de imagini accesat	Extragere efectuată	Destinatarul secvenței extrase	Semnătura

Anexa nr. 5
la Regulamentul privind instalarea și
utilizarea sistemelor de supraveghere video
în instituțiile de educație timpurie

Lista minimă a documentelor din dosarul de fundamentare

1. Nota de fundamentare privind necesitatea instalării sistemului
2. Analiza măsurilor alternative
3. Evaluarea impactului asupra protecției datelor, după caz
4. Planul de amplasare a camerelor
5. Descrierea câmpului vizual al fiecărei camere
6. Proiectul pictogramelor și al notei informative
7. Procedura de stocare și ștergere
8. Lista funcțiilor cu acces la imagini
9. Descrierea măsurilor tehnice și organizatorice de securitate
10. Avizul responsabilului cu protecția datelor sau al persoanei desemnate
11. Aprobarea fondatorului
12. Contractul cu prestatorul, după caz

Anexa nr. 6
la Regulamentul privind instalarea și
utilizarea sistemelor de supraveghere video
în instituțiile de educație timpurie

***Modele de acte și documente aferente dosarului de fundamentare pentru instalarea și
utilizarea sistemelor de supraveghere video în instituțiile de educație timpurie***

Prezenta anexă conține modele orientative de acte și documente care pot fi utilizate de instituțiile de educație timpurie și de fondatori la întocmirea, examinarea și aprobarea dosarului de fundamentare.

Secțiunea 1

Model de Notă de fundamentare privind necesitatea instalării sistemului de supraveghere video

Denumirea instituției: _____

Adresa: _____

Fondatorul: _____

Data: _____

Nr. de înregistrare: _____

NOTĂ DE FUNDAMENTARE

privind necesitatea instalării sistemului de supraveghere video

1. Obiectul propunerii

Prezenta notă de fundamentare este întocmită în vederea justificării necesității instalării și utilizării sistemului de supraveghere video în cadrul Instituției de Educație Timpurie

2. Scopul urmărit

Instalarea sistemului este propusă în vederea realizării următoarelor scopuri:

- a) asigurarea securității copiilor, personalului și vizitatorilor;
- b) prevenirea și clarificarea incidentelor ce pot afecta siguranța persoanelor;
- c) protejarea bunurilor și patrimoniului instituției;
- d) controlul accesului în instituție și în anumite spații ale acesteia;
- e) documentarea incidentelor de securitate, conflict, violență sau accident.

3. Situația de fapt și problemele identificate

Se descriu succint circumstanțele concrete care justifică necesitatea instalării sistemului, inclusiv numărul și tipologia incidentelor înregistrate, riscurile specifice identificate la nivelul instituției, vulnerabilitățile legate de acces, perimetru, circulație internă, bunuri sau siguranța copiilor, precum și sesizările, constatările sau rapoartele relevante.

4. Justificarea necesității

Se motivează de ce instituirea supravegherii video este necesară pentru atingerea scopului urmărit și de ce riscurile identificate nu pot fi gestionate în mod suficient prin alte măsuri mai puțin intruzive.

5. Justificarea proporționalității

Se arată de ce măsura este limitată la spațiile strict necesare, de ce sistemul nu depășește ceea ce este necesar pentru atingerea scopului și ce garanții vor fi aplicate pentru protejarea vieții private și a datelor cu caracter personal.

6. Spațiile propuse pentru supraveghere

Se indică spațiile concrete în care se propune instalarea camerelor și justificarea fiecărui spațiu.

7. Garanții și măsuri de protecție

Se menționează cel puțin lipsa captării audio, interzicerea recunoașterii faciale sau a altor funcții biometrice, limitarea accesului la imagini, termenul de retenție, procedura de ștergere și informarea persoanelor vizate.

8. Concluzie

În temeiul celor expuse, se propune aprobarea instalării sistemului de supraveghere video în condițiile descrise în prezenta notă și în documentele anexate.

Director: _____

Semnătura: _____

Secțiunea 2

Model de Analiză a măsurilor alternative

Denumirea instituției: _____

ANALIZA MĂSURILOR ALTERNATIVE

la instalarea sistemului de supraveghere video

1. Scopul analizei

Prezenta analiză este întocmită pentru a demonstra dacă scopurile urmărite de instituție pot fi atinse prin măsuri alternative mai puțin intruzive decât supravegherea video.

2. Măsuri alternative examinate

Nr.	Măsura alternativă	Rezultate/grad de eficiență	Motivul pentru care nu este suficientă
1	Pază umană		
2	Control acces		
3	Iluminare suplimentară		
4	Alte măsuri		

3. Concluzii

În urma analizei, se constată dacă măsurile alternative examinate pot atinge integral scopurile urmărite sau dacă acestea pot fi menținute doar complementar, fără a substitui necesitatea unui sistem de supraveghere video.

Director: _____

Semnătura: _____

Secțiunea 3

Model de Evaluare a impactului asupra protecției datelor

EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR

(model orientativ)

1. Date generale

1. Denumirea operatorului: _____

2. Adresa: _____

3. Reprezentant legal: _____

4. Responsabil cu protecția datelor/persoană desemnată:

5. Data evaluării: _____

2. Descrierea prelucrării

1. Scopurile prelucrării: _____

2. Categoriile de persoane vizate: copii, părinți/reprezentanți legali, angajați, vizitatori, alți terți.

3. Categoriile de date: imagini video, data și ora înregistrării, localizarea camerei.

4. Zonele supravegheate: _____

5. Durata stocării: _____

6. Destinatarii imaginilor: _____

7. Prestatori implicați: _____

3. Temeiul și justificarea

Se descriu scopul legitim, necesitatea măsurii, proporționalitatea măsurii și inexistența unor alternative suficiente.

4. Analiza riscurilor pentru drepturile și libertățile persoanelor vizate

Nr.	Riscul identificat	Nivelul riscului	Măsuri de reducere
1	Acces neautorizat la imagini		
2	Supraveghere excesivă		
3	Captare a unor zone nepermise		
4	Divulgare neautorizată		

5. Măsuri de diminuare a riscurilor

Se indică limitarea spațiilor supravegheate, lipsa captării audio, accesul restricționat și jurnalizat, retenția limitată, ștergerea automată, instruirea personalului, semnalizarea și informarea, precum și procedurile de răspuns la cereri și incidente.

6. Concluzia evaluării

☐ riscurile sunt acceptabile în condițiile măsurilor propuse;

☐ sunt necesare măsuri suplimentare;

☐ proiectul nu poate fi implementat în forma propusă.

Responsabil cu protecția datelor/persoană desemnată: _____

Semnătura: _____

Director: _____

Semnătura: _____

Secțiunea 4

Model de Plan de amplasare a camerelor

PLAN DE AMPLASARE A CAMERELOR

Denumirea instituției: _____

Nr. camere	Denumirea spațiului	Categoria spațiului	Scopul supravegherii	Poziția camerei / observații
1				
2				

Instrucțiuni de completare:

La plan se anexează obligatoriu schița sau planul instituției, cu marcarea exactă a poziției fiecărei camere și a direcției generale de captare.

Director: _____

Semnătura: _____

Secțiunea 5

Model de Descriere a câmpului vizual al fiecărei camere

DESCRIEREA CÂMPULUI VIZUAL AL FIECĂREI CAMERE

Denumirea instituției: _____

Nr. camerei	Spațiul supravegheat	Ce se captează	Ce nu se captează	Unghi/orientare și justificare
1				
2				
3				

Mențiuni obligatorii:

1. Nu se admit descrieri generale fără delimitare exactă.
2. Se menționează expres dacă există captare incidentală inevitabilă a unei zone marginale.
3. Se menționează expres că nu se captează zone interzise.

Director: _____

Semnătura: _____

Responsabil cu protecția datelor / persoană desemnată: _____

Secțiunea 6

Model de Proiect al pictogramelor și al notei informative

A. Model de pictogramă

• Atenție! Zonă supravegheată video

Scop: asigurarea securității copiilor, a personalului și a bunurilor instituției.

Operator: IET „_____”

Date de contact: _____

Responsabil cu protecția datelor/persoană desemnată: _____

Informații complete sunt disponibile la sediul instituției și/sau pe pagina web.

B. Model de notă informativă completă

1. Operatorul de date: _____
2. Scopurile supraveglierii video: _____
3. Zonele supravegheate: _____
4. Temeiul prelucrării: _____
5. Termenul de stocare: _____
6. Destinatarii sau categoriile de destinatari ai imaginilor: _____
7. Drepturile persoanelor vizate: _____
8. Modalitatea de exercitare a drepturilor: _____

9. Date de contact pentru solicitări: _____

Secțiunea 7

Model de Procedură de stocare și ștergere a imaginilor

PROCEDURA

de stocare și ștergere a imaginilor video

1. Dispoziții generale

Prezenta procedură stabilește modul de stocare, accesare, extragere și ștergere a imaginilor video obținute prin sistemul de supraveghere video al IET _____.

2. Stocarea imaginilor

- (1) Imaginile se stochează pe suportul/sistemul: _____.
- (2) Accesul la sistemul de stocare este permis numai persoanelor autorizate.
- (3) Sistemul este configurat pentru ștergerea automată a imaginilor la expirarea termenului de retenție.

3. Termenul de retenție

- (1) Imaginile se păstrează pe o perioadă de ____ zile calendaristice.
- (2) În cazul producerii unui incident, se extrage și se păstrează separat numai secvența relevantă.

4. Extragerea imaginilor

- (1) Extragerea imaginilor se face numai de persoanele autorizate.
- (2) Extragerea se consemnează în registrul de acces și într-un proces-verbal.
- (3) Se extrage numai secvența strict necesară.

5. Ștergerea imaginilor

- (1) Ștergerea imaginilor din fluxul curent se realizează automat și definitiv.
- (2) Secvențele extrase se șterg la încetarea temeiului care a justificat păstrarea lor.

6. Responsabilități

Directorul și persoana desemnată asigură respectarea prezentei proceduri.

Director: _____

Semnătura: _____

Secțiunea 8

Model de Listă a funcțiilor cu acces la imagini

LISTA FUNCȚIILOR CU ACCES LA IMAGINI

În cadrul IET _____, acces la imaginile obținute prin sistemul de supraveghere video au doar următoarele funcții:

Nr.	Funcția	Tipul accesului	Scopul accesului / observații
1	Director	complet/limitat	administrare, incidente

2	Responsabil protecția datelor / persoană desemnată	complet/limitat	conformitate, evidență
3	Altă funcție autorizată	complet/limitat	

Mențiune:

Accesul se acordă în baza actului intern de desemnare și numai în limita atribuțiilor de serviciu.

Director: _____

Semnătura: _____

Secțiunea 9

Model de Descriere a măsurilor tehnice și organizatorice de securitate

DESCRIEREA MĂSURILOR TEHNICE ȘI ORGANIZATORICE DE SECURITATE

Denumirea instituției: _____

1. Măsuri tehnice

- a) protejarea sistemului prin parolă și autentificare individuală;
- b) limitarea accesului la rețea și la sistem;
- c) jurnalizarea accesului;
- d) sincronizarea datei și orei;
- e) backup controlat, dacă este cazul;
- f) protecție antivirus/antimalware, după caz;
- g) actualizarea periodică a software-ului/firmware-ului;
- h) dezactivarea funcțiilor audio și biometrice;
- i) criptare, dacă este disponibilă și aplicabilă.

2. Măsuri organizatorice

- a) desemnarea persoanelor autorizate;
- b) instruirea periodică a personalului;
- c) semnarea angajamentelor de confidențialitate;
- d) procedură privind cererile de acces la imagini;
- e) procedură privind incidentele de securitate;
- f) revizuire periodică a necesității sistemului;
- g) control intern și audit anual.

3. Concluzii

Măsurile descrise asigură un nivel adecvat de protecție raportat la riscurile identificate.

Responsabil cu protecția datelor / persoană desemnată: _____

Semnătura: _____

Secțiunea 10

Model de Aviz al responsabilului cu protecția datelor sau al persoanei desemnate

AVIZ

al responsabilului cu protecția datelor / persoanei desemnate

Subsemnatul(a) _____, în calitate de responsabil cu protecția datelor / persoană desemnată în cadrul IET _____, examinând dosarul de fundamentare privind instalarea sistemului de supraveghere video, constat următoarele:

1. Dosarul conține / nu conține documentele necesare.
2. Scopul propus este / nu este determinat și legitim.
3. Necesitatea și proporționalitatea măsurii sunt / nu sunt suficient justificate.
4. Spațiile propuse sunt / nu sunt conforme cu prezenta Instrucțiune.
5. Măsurile de protecție a datelor sunt / nu sunt suficiente.
6. Evaluarea impactului asupra protecției datelor este / nu este necesară și a fost / nu a fost efectuată.

Aviz:

☐ favorabil

☐ favorabil cu recomandări

☐ nefavorabil

Recomandări / observații:

Data: _____

Nume și prenume: _____

Semnătura: _____

Secțiunea 11

Model de Aprobare a fondatorului

APROBAREA FONDATORULUI

Examinând dosarul de fundamentare prezentat de IET _____, inclusiv nota de fundamentare, analiza măsurilor alternative, evaluarea impactului asupra protecției datelor, avizul responsabilului cu protecția datelor / persoanei desemnate și celelalte acte anexate, fondatorul decide:

☐ aprobă instalarea sistemului de supraveghere video, în condițiile descrise în dosar;

☐ aprobă instalarea sistemului de supraveghere video, cu următoarele condiții suplimentare:

[] respinge propunerea, din următoarele motive:

Data: _____

Funcția: _____

Nume și prenume: _____

Semnătura și ștampila, după caz: _____

Secțiunea 12

Model de clauze minime pentru Contractul cu prestatorul, după caz

CLAUZE MINIME

pentru contractul cu prestatorul de instalare/mentenanță/stocare

1. Părțile contractante

Beneficiar: IET _____

Prestator: _____

2. Obiectul contractului

Prestatorul va asigura, după caz:

- a) instalarea sistemului de supraveghere video;
- b) configurarea echipamentelor și a aplicațiilor;
- c) mentenanța tehnică;
- d) stocarea externă, dacă este cazul;
- e) asistența tehnică.

3. Limitele prelucrării

Prestatorul prelucrează datele numai în baza instrucțiunilor documentate ale beneficiarului și exclusiv în scopul executării contractului.

4. Confidențialitatea

Prestatorul și personalul său au obligația de a păstra confidențialitatea datelor și a imaginilor la care au acces.

5. Interdicția utilizării în scop propriu

Prestatorul nu are dreptul să utilizeze, copieze, transmită, divulge sau valorifice imaginile în scop propriu ori în interesul altor persoane.

6. Măsuri de securitate

Prestatorul aplică măsuri tehnice și organizatorice adecvate pentru protejarea datelor împotriva accesului neautorizat, divulgării, modificării, pierderii sau distrugerii.

7. Accesul tehnic

Orice acces tehnic la sistem se realizează numai cu aprobarea beneficiarului și se consemnează.

8. Subcontractarea

Prestatorul nu poate subcontracta operațiuni care implică acces la date fără acordul prealabil scris al beneficiarului.

9. Incident de securitate

Prestatorul notifică imediat beneficiarul despre orice incident de securitate sau acces neautorizat la date.

10. Încetarea contractului

La încetarea contractului, prestatorul returnează sau șterge toate datele și imaginile, conform instrucțiunilor beneficiarului.

11. Răspunderea

Prestatorul răspunde pentru încălcarea obligațiilor contractuale și legale privind protecția datelor și confidențialitatea.