



JUDECĂTORIA CIMIȘLIA

REGULAMENT

**privind utilizarea și securitatea sistemului
de control acces (turnichet)
în cadrul Judecătoriei Cimișlia**

APROBAT:

Președintă interimară a Judecătoriei Cimișlia



Veronica CARAPIREA
prin Ordinul nr. 47 din 29 octombrie 2025

Capitolul I. Dispoziții generale

1.1. Presentul Regulament stabilește modul de utilizare, administrare și securitate a sistemului de control acces (turnichet) dotat cu sistem de recunoaștere facială („face control”), instalat în cadrul Judecătoriei Cimișlia, în vederea asigurării securității persoanelor, bunurilor și informațiilor, precum și a respectării cerințelor legale privind protecția datelor cu caracter personal.

Capitolul II. Scopul și temeiul legal

2.1. Sistemul de control acces este implementat pentru:

- a) controlul intrărilor și ieșirilor în incinta instanței;
- b) prevenirea accesului neautorizat;
- c) asigurarea evidenței prezenței personalului;
- d) protejarea patrimoniului instituției.

2.2. Temeiul legal al prelucrării datelor cu caracter personal îl constituie:

- [Legea nr. 514-XIII din 06 iulie 1995 cu privire la organizarea judecătorească;](#)
- [Legea nr. 544-XIII din 20 iulie 1995 cu privire la statutul judecătorului;](#)
- [Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal;](#)
- [Hotărârea Guvernului nr. 201/2017 privind cerințele minime obligatorii de securitate cibernetică;](#)
- [Legea nr. 142 din 19.07.2018 privind schimbul de date și interoperabilitate;](#)
- [Hotărârii Guvernului nr. 701 din 11 iulie 2018 pentru aprobarea Regulamentului privind protecția antiteroristă a infrastructurii critice;](#)
- [Hotărârii Guvernului nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;](#)
- [Regulile de conduită a justițiabililor și altor persoane în instanța judecătorească, aprobate prin Hotărârea Consiliului Superior al Magistraturii nr. 504/17 din 03 iunie 2014.](#)
- [Actele normative interne ale sistemului judecătoresc privind securitatea informațională și protecția datelor.](#)

Capitolul III. Tipurile de date prelucrate

3.1. În cadrul sistemului de control acces (turnichet) se colectează și se prelucrează următoarele date:

- a) nume și prenume ale persoanei;
- b) număr de identificare al cardului de acces;
- c) imagine facială criptată (șablon biometric);
- d) data și ora accesului;
- e) punctul fizic de intrare/ieșire.

3.2. Datele biometrice sunt stocate în format criptat și nu pot fi utilizate în scopuri de identificare vizuală, ci doar pentru autentificare automată în cadrul sistemului de acces.

Capitolul IV. Modul de stocare și păstrare a datelor

Programul de administrare a sistemului de control acces (iVMS-4200)

4.1. Datele colectate de sistem sunt stocate atât local, în memoria controlerului turnichetului, cât și Programul de administrare a sistemului de control acces (iVMS-4200) al Judecătoriei Cimișlia, care va cuprinde elemente precum:

- Denumirea aplicației și scopul utilizării ei;
- Tipurile de informații prelucrate prin program (date de acces, imagini faciale, jurnale de evenimente);
- Termenele de stocare (loguri 6 luni, evenimente 1 an), după care acestea se șterg automat sau se anonimizează.
- Măsuri de securitate aplicate la nivel de sistem;
- Controlul accesului la interfața de administrare (doar personal autorizat IT / desemnat de președinte Judecătoriei Cimișlia prin Ordinul nr. 21 din 31.01.2025);
- Modul de export și ștergere a datelor;
- Respectarea cadrului legal privind protecția datelor personale.

4.2. Capacitatea de stocare locală este de aproximativ 100 000 de evenimente.

4.3. Backup-ul datelor se efectuează lunar pe un suport securizat, aflat în administrarea specialistilor desemnați de președinte Judecătoriei Cimișlia prin ordin.

4.4. Comunicarea între turnichet și programul instituției se realizează prin conexiune criptată și autentificată.

4.5. Datele nu se transmit către terți și nu se utilizează în alte scopuri decât cele prevăzute de prezentul Regulament.

Capitolul V. Accesul la date și măsuri de securitate

5.1. Accesul la datele generate de sistemul de control acces îl au doar persoanele desemnate de președintele instanței prin ordin.

5.2. Fiecare utilizator al sistemului de administrare dispune de credențiale individuale (nume utilizator și parolă unică).

5.3. Toate acțiunile efectuate în sistem sunt înregistrate automat în jurnalul de audit.

5.4. Echipamentele sistemului sunt amplasate în spații securizate, protejate fizic și electronic, conform Planului de amplasare (*anexa nr. 2*).

5.5. Este interzisă extragerea, copierea sau transmiterea datelor fără aprobarea scrisă a președintelui instanței.

5.6. În caz de incident de securitate, se aplică imediat procedura internă de notificare și, dacă este cazul, informarea Autorității Naționale pentru Protecția Datelor cu Caracter Personal în termen de 72 de ore.

Capitolul VI. Drepturile persoanelor vizate

6.1. Persoanele ale căror date sunt prelucrate prin intermediul sistemului de turnichet au dreptul:

- a) să fie informate cu privire la prelucrarea datelor lor;
- b) să solicite accesul la datele proprii;
- c) să ceară rectificarea sau restricționarea prelucrării datelor, în limitele legii;
- d) să se adreseze Autorității Naționale pentru Protecția Datelor cu Caracter Personal în caz de încălcare a drepturilor.

Capitolul VII. Responsabilități

7.1. Președintele Judecătorei Cimișlia asigură implementarea și respectarea prezentului Regulament.

7.2. Specialiștii desemnați prin ordin sunt responsabili de întreținerea tehnică, securitatea și funcționarea corectă a sistemului de control acces.

7.3. Responsabilul pentru protecția datelor (DPO) monitorizează respectarea cerințelor Legii nr. 133/2011 și informează conducerea despre eventualele riscuri.

7.4. Angajații au obligația de a respecta procedurile stabilite și de a nu divulga datele obținute prin intermediul sistemului.

Capitolul VIII. Specificațiile tehnice

8.1. **Turnichet tripod:** MTBF > 3.000.000 de cicluri. Memorie pentru 500.000 de carduri de acces, 500.000 de evenimente.

- Lățime pasaj protejat: 55 cm.
- Sistemul inteligent de control va revoca permisiunea de acces dacă o persoană nu trece prin turnichet în timpul alocat.
- Indicator LED intrare/ieșire.
- Debit mediu: 35 de persoane pe minut.
- Cititoare de carduri Mifare încorporate.
- Control și gestionare de la distanță. Moduri de acces liber sau restricționat. Mod anti-panică: când se declanșează o alarmă de incendiu, brațele turnichetului coboară automat pentru evacuarea de urgență.
- Conectarea cititoarelor și controlerelor terțe prin RS-485. Receptor radio încorporat pentru telecomandă. Suport pentru protocolul ISAPI pentru integrarea cu sisteme de gestionare software terțe.
- Material carcasă: oțel inoxidabil SUS304. Alimentare: 100 - 240 VAC. Utilizare în interior. Interval de temperatură: -10°C până la 45°C. Dimensiuni: 502 x 202 x 1010 mm. Garanție de un an!

8.2. **Terminal de acces biometric multifactor și pontaj bazat pe recunoaștere facială:**

Suportă integrarea cu sistemele de interfonie IP (apelarea abonaților de la terminal). Identificare prin față, sau card.

- Obiectiv dual cu unghi larg și rezoluție de 2 MP. Rază de recunoaștere: 0,3 - 1,5 m. Viteză de recunoaștere facială: 0,2 sec.
- Bază de date cu 1.500 de fețe.
- Ecran tactil de 4,3 inci cu o rezoluție de 480×272 pixeli.
- Comunicare audio bidirecțională prin microfon și difuzor încorporate.
- Cititor de carduri de acces Mifare încorporat (până la 3.000 de carduri).
- Interfețe: LAN, 1 x RS-485, 1 x Wiegand, 1 x USB 2.0. Memorie pentru 150.000 de evenimente. Protecție împotriva spoofing-ului facial.
- Deschiderea ușii de la distanță și vizualizare în timp real prin Hik-Connect. Sistem de operare Linux.
- Funcționare independentă posibilă.

Capitolul IX – Programul de administrare a sistemului de control acces (iVMS-4200)

9.1. Programul de administrare a sistemului de control acces (iVMS-4200), va cuprinde elemente precum:

- Denumirea aplicației și scopul utilizării ei;
- Tipurile de informații prelucrate prin program (date de acces, imagini faciale, jurnale de evenimente);
- Termenele de stocare (loguri 6 luni, evenimente 1 an);
- Măsuri de securitate aplicate la nivel de sistem;
- Controlul accesului la interfața de administrare (doar personalul desemnat de președinte Judecătoriei Cimișlia prin Ordinul nr. 21 din 31.01.2025);
- Modul de export și ștergere a datelor;
- Respectarea cadrului legal privind protecția datelor personale.

Capitolul X - Instructaj

10.1. Persoanele desemnate de președinte Judecătoriei Cimișlia cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor.

10.2. 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 prin mijloace video.

10.3. Șefii subdiviziunilor instanței vor asigura că întregul personal din subordine, este instruit și informat cu privire la toate aspectele funcționale, operaționale și administrative ale acestei activități.

Capitolul XI- Informarea publicului referitor la supravegherea video

11.1. Informarea publicului referitor la sistemului de control acces (turnichet) din cadrul Judecătoriei Cimișlia se efectuează prin pictograme, conform modelului prevăzut în **anexa nr. 1**.

11.2. Judecătoria Cimișlia garantează asigurarea respectării drepturilor ce le revin persoanelor vizate, în conformitate cu legislația în vigoare.

11.3. Toate persoanele implicate în activitatea sistemului de control acces (turnichet) și cele responsabile de administrarea datelor, vor respecta procedurile și regulamentele Judecătoriei Cimișlia care se referă la accesul la datele cu caracter personal și semnează un angajament de confidențialitate (**anexa nr. 3**)

Capitolul XII. Răspunderea și sancțiuni

12.1. Încălcarea prevederilor prezentului Regulament atrage răspunderea disciplinară, civilă sau penală, conform legislației în vigoare. Orice prelucrare neautorizată a datelor cu caracter personal este interzisă și sancționată potrivit art. 33 din Legea nr. 133/2011.

Capitolul XIII. Dispoziții finale

13.1. Prezentul Regulament intră în vigoare la data aprobării prin Ordin al Președintelui interimar al Judecătoriei Cimișlia.

13.2. Toți angajații și persoanele care utilizează sistemul de control acces vor lua cunoștință de conținutul acestuia sub semnătură.

Elaborat de șefă a secretariatului

Natalia MICULICI

(anexa nr. 1)

la Regulamentul privind utilizarea și securitatea
sistemului de control acces (turnichet)
în cadrul Judecătoriei Cimișlia



APROBAT
prin Ordin nr. 47
din 29.10.2025
președinte interimar

Veronica CARAPIREA

AVIZ DE INFORMARE

Conform Legii nr. 133/2011 privind protecția datelor cu caracter personal, vă informăm că accesul în incinta Judecătoriei Cimișlia se realizează prin intermediul unui sistem de control acces (turnichet) dotat cu recunoaștere facială.

Datele colectate (imagine facială, nume, oră, punct acces) sunt utilizate exclusiv pentru scopuri de securitate și control acces.

Operator de date: Judecătoria Cimișlia.

- Datele se păstrează timp de 12 luni și nu se transmit terților.

Pentru exercitarea drepturilor dumneavoastră privind datele personale, vă puteți adresa responsabilului desemnat de președinte Judecătoriei Cimișlia prin Ordinul nr. 21 din 31.01.2025.

(anexa nr. 2)



la Regulamentul privind utilizarea și securitatea
sistemului de control acces (turnichet)
în cadrul Judecătoriai Cimișlia

APROBAT

prin Ordin nr. 47

din 29.10.2025

președinte interimar

Veronica CARAPIREA

PLAN SCHEMĂ A LOCALIZĂRII sistemului de control acces (turnichet) în cadrul Judecătoriai Cimișlia

- 1 ▲ Turnichet tripod/ Terminal de acces biometric multifactor și pontaj bazat pe recunoaștere facială- **Intrarea prin ușa din față, în holul instanței;**
- 2 ▲ Terminal de acces biometric multifactor și pontaj bazat pe recunoaștere facială- **Intrarea din spate instanței, folosită în caz de situații excepționale.**



(anexa nr. 3)

la Regulamentul privind utilizarea și securitatea
sistemului de control acces (turnichet)
în cadrul Judecătoriei Cimișlia

APROBAT

prin Ordin nr. 47

din 29.10.2025

președinte interimar

Veronica CARAPIREA



Angajament scris de confidențialitate

Eu, [numele, prenumele], angajat al Judecătoriei Cimișlia, cu funcția de [indicați funcția], înțeleg și accept următoarele prevederi referitoare la utilizarea sistemului de control acces (turnichet):

1. Mă angajez să respect confidențialitatea și securitatea datelor cu caracter personal prelucrate prin intermediul sistemului de control acces (turnichet).
2. Înțeleg că accesul la datele înregistrate și la arhitectura tehnică a sistemului de control acces (turnichet) este limitat cu scopul de a asigura confidențialitatea, integritatea și securitatea datelor cu caracter personal, precum și protecția drepturilor individuale ale persoanelor aflate sub supraveghere.
3. Sunt conștient de faptul că utilizarea în timp real este permisă doar personalului cu funcții de asigurare al securității fizice și control acces, iar vizualizarea înregistrărilor se vor face doar în cazuri justificate, conform prevederilor legale și în circumstanțe prevăzute de regulament.
4. Mă oblig să nu copiez, să nu descarc, să nu șterg sau să nu modific în nici un înscris din sistemului de control acces (turnichet), fără aprobarea corespunzătoare din partea conducerii Judecătoriei Cimișlia.
5. Sunt conștient de faptul că dezvăluirea datelor personale către terți este permisă doar cu acordul scris al președintelui, iar în absența acestuia, a vicepreședintelui Judecătoriei Cimișlia.
6. Prin semnarea acestui angajament, declar că am citit și înțeles prevederile acestuia și mă angajez să respect în mod corespunzător toate obligațiile și restricțiile impuse în legătură cu utilizarea sistemului de control acces (turnichet).

Data: _____

Semnătura: _____