

Anexa nr.1
la Hotărârea Guvernului
nr.____din_____2022

CONCEPTUL

Sistemului informațional de supraveghere video portabil „Camera de corp”

Capitolul I

INTRODUCERE

Conceptul Sistemului informațional de supraveghere video portabil „Camera de corp” a fost elaborat de către Ministerul Afacerilor Interne ca urmare a promovării și implementării principiului de „*toleranță zero*” față de corupție, ce constă în fortificarea capacității de prevenire și combatere a comportamentului corupt în cadrul autorităților administrative și instituțiilor din subordine.

Conceptul precitat a fost elaborat în temeiul articolelor 16, 22 lit. c) și d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat.

Scopul Conceptului Sistemului informațional de supraveghere video portabil „Camera de corp” este de a asigura suportul informațional al activității Ministerului Afacerilor Interne, precum și reducerea semnificativă a corupției în rândul angajaților din subordine.

Camerele video sunt utilizate pentru protejarea angajaților Ministerului Afacerilor Interne, precum și în vederea sporii profesionalismului, prin analiza deficiențelor activității funcționarului public cu statut special/militar în timpul serviciului în baza înregistrărilor video. Totodată, înregistrările video pot fi utilizate în calitate de probă/mijloace materiale de probă pentru constatarea existenței sau inexistenței contravenției/infracțiunii sau a abaterilor disciplinare.

Implementarea Sistemului informațional sus indicat va contribui la sporirea gradului de transparență a activității Ministerului Afacerilor Interne, prevenirea și monitorizarea conflictelor dintre persoane, inclusiv, străine și angajații din subordine, prevenirea corupției, incidentelor de utilizare abuzivă a forței fizice și a mijloacelor speciale în timpul îndeplinirii atribuțiilor de serviciu.

Sistemul informațional prenotat va înlesni creșterea responsabilității și a profesionalismului funcționarilor publici cu statut special/militar în timpul exercitării atribuțiilor de serviciu, consolidarea capacității de prevenire și combatere a comportamentului corupt în cadrul autorităților administrative și instituțiilor din subordinea Ministerului Afacerilor Interne, sporirea nivelului de disciplină al angajaților, responsabilizării persoanelor etc.

Prezentul concept stabilește obiectivele, scopul, principiile, cadrul normativ-juridic, caracteristicile funcționale de bază și arhitectura conceptuală a Sistemului informațional, precum și descrie obiectivele informaționale și funcționalitățile acestuia.

Capitolul II DISPOZIȚII GENERALE

1. Sistemul informațional de supraveghere video portabil „Camera de corp”, (în continuare - Sistem informațional) constituie totalitatea resurselor și tehnologiilor informaționale, mijloacelor tehnice de program și metodologiilor aflate în interconexiune și destinate înregistrării, procesării, păstrării, prelucrării și utilizării informațiilor audio, foto și video.

2. Noțiunile utilizate în prezentul Concept sunt definite în Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat.

De asemenea, în sensul prezentului Concept se utilizează următoarele noțiuni:

cameră de corp – ansamblu de echipamente constituit din unitate de captare video portabilă și alte accesorii aferente, configurate potrivit parametrilor tehnici ce asigură înregistrarea video, audio, foto și localizarea prin sistemul de recepționare globală (în continuare – GPS);

stație de andocare – unitate de descărcare a înregistrărilor video, audio, foto și de alimentare a camerelor de corp;

stocare – păstrarea pe orice fel de suport a datelor Sistemului informațional;

utilizator – autoritățile administrative și instituțiile din subordinea Ministerului Afacerilor Interne.

3. Sistemul informațional este destinat să garanteze desfășurarea activității Ministerului Afacerilor Interne conform legislației, în interesul persoanei și al comunității, potrivit principiilor profesionalismului, confidențialității, integrității profesionale și loialității, colaborării și cooperării, imparțialității și nediscriminării, transparenței, obiectivității, eficienței și responsabilității.

4. Prin crearea Sistemului informațional se urmărește atingerea următoarelor obiective:

1) creșterea nivelului de protecție a drepturilor și libertăților persoanei, precum și a angajaților Ministerului Afacerilor Interne;

2) sporirea nivelului de protecție și asigurare a securității angajaților Ministerului Afacerilor Interne în timpul exercitării atribuțiilor de serviciu;

3) creșterea încrederii societății în Ministerul Afacerilor Interne și îmbunătățirea reputației acestuia;

4) responsabilizarea angajaților Ministerului Afacerilor Interne și al persoanelor;

5) sporirea transparenței activității Ministerului Afacerilor Interne;

6) prevenirea și reducerea corupției;

7) sporirea profesionalismului și stimularea angajaților Ministerului Afacerilor Interne să acționeze în conformitate cu actele normative;

8) prevenirea aplicării nejustificate și reducerea incidentelor de utilizare abuzivă a forței fizice, a mijloacelor speciale și a armelor de foc de către angajații Ministerului Afacerilor Interne;

9) identificarea deficiențelor activității angajaților Ministerului Afacerilor Interne în timpul turei/serviciului;

10) utilizarea înregistrărilor fixate de camerele de corp ca probă/mijloc de probă.

5. Scopul implementării Sistemului informațional este realizarea unui serviciu profesionist, eficient, care va determina exercitarea atribuțiilor funcționale în interesul persoanei și al comunității, asigurând respectarea legii, a drepturilor și libertăților fundamentale ale omului, precum și protecția juridică a angajaților Ministerului Afacerilor Interne.

6. Principiile de bază ale Sistemului informațional sunt:

1) *principiul legalității*, care prevede crearea și exploatarea Sistemului informațional în conformitate cu legislația;

2) *principiul respectării drepturilor omului*, care prevede exploatarea Sistemului informațional în strictă corespundere cu actele normative naționale, tratatele și convențiile internaționale privind drepturile omului la care Republica Moldova este parte;

3) *principiile integrității, plenitudinii și veridicității datelor*, ce reflectă starea în care datele își păstrează conținutul și interpretarea uniformă în anumite situații neprevăzute, în corespundere cu documentele normative și obiectul real al evidenței;

4) *principiul identificării de stat*, care prevede atribuirea fiecărui obiect al înregistrării unui număr de identificare;

5) *principiul dirijării formării și utilizării Sistemului informațional*, care reprezintă o totalitate de măsuri organizatorice și tehnice de program ce asigură calitatea înaltă a resurselor informaționale de stat formate, fiabilitatea înaltă a stocării lor și corectitudinea utilizării în corespundere cu legislația, precum și care mențin accesul operativ și comod la informație, în limitele competenței stabilite de legislație și nivelul lui de acces;

6) *principiul confidențialității informației*, care prevede răspunderea personală, în conformitate cu legislația, a angajaților Ministerului Afacerilor Interne responsabili de prelucrarea informației în Sistemul informațional, pentru utilizarea și difuzarea neregulamentară a informației;

7) *principiul securității informaționale*, care presupune asigurarea integrității, exclusivității, accesibilității și eficienței protecției datelor, inclusiv a datelor cu caracter personal împotriva pierderii, denaturării, deteriorării și utilizării neautorizate. Securitatea Sistemului informațional presupune rezistența la atacuri și protecția caracterului secret, integrității și pregătirii pentru lucru atât a Sistemului informațional, cât și a datelor lui;

8) *principiul compatibilității Sistemului informațional cu sistemele existente în țară*;

9) *principiul extinderii Sistemului informațional în perspectivă asupra noilor obiecte*;

10) *principiul scalarității*, ce prevede utilizarea mărimilor ale căror valori sunt determinate numai prin unități de măsură și numere reale, care nu depind de vreun sistem de referință.

Capitolul III

CADRUL NORMATIV-JURIDIC AL SISTEMULUI INFORMAȚIONAL

7. Crearea și funcționarea Sistemului informațional este reglementată de următoarele acte normative:

Constituția Republicii Moldova;

Codul penal al Republicii Moldova nr.985/2002;

Codul de procedură penală al Republicii Moldova nr.122/2003;

Codul contravențional al Republicii Moldova nr.218/2008;

Legea nr.982/2000 privind accesul la informație;

Legea nr.1069/2000 cu privire la informatică;

Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;

Legea nr.241/2007 comunicațiilor electronice;

Legea nr.93/2007 Inspectoratului General pentru Situații de Urgență;

Legea nr.133/2011 privind protecția datelor cu caracter personal;

Legea nr.283/2011 cu privire la Poliția de Frontieră;

Legea nr.59/2012 privind activitatea specială de investigații;

Legea nr.320/2012 cu privire la activitatea Poliției și statutul polițistului;

Legea nr.142/2018 cu privire la schimbul de date și interoperabilitate;

Legea nr.219/2018 cu privire la Inspectoratul General de Carabinieri;

Hotărârea Guvernului nr. 1032/2006 cu privire la aprobarea Concepției sistemului informațional automatizat „Registrul resurselor și sistemelor informaționale de stat”;

Hotărârea Guvernului nr. 1202/2006 cu privire la aprobarea Concepției Sistemului informațional integrat al organelor de drept;

Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;

Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;

Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;

Standardele Republicii Moldova:

a) SM ISO/CEI 15288:2015 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului”;

b) SM ISO/CEI 12207:2014 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”;

c) SM ISO/CEI 27002:2014 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației”;

d) SM ISO/CEI 15408-1 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 1: Introducere și model general”;

e) SM ISO/CEI 15408-2 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 2: Cerințe funcționale de securitate”;

f) SM ISO/CEI 15408-3 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 3: Cerințe de asigurare a securității”;

alte acte normative.

Capitolul IV

SPAȚIUL FUNCȚIONAL

AL SISTEMULUI INFORMAȚIONAL

8. Funcțiile de bază ale Sistemului informațional sunt următoarele:

1) înregistrare – reflectarea video, audio și/sau foto a informațiilor despre interacțiunile/evenimentele în care sunt implicați angajații Ministerului Afacerilor Interne în timpul executării serviciului;

2) localizare prin sistem de recepționare globală (GPS) – reflectarea datelor geospațiale cu referire la localizarea angajatului Ministerului Afacerilor Interne dotat cu cameră de corp;

3) alarmă – transmiterea semnalului de alarmă către unitatea centrală de procesare și gestionare (software);

4) luarea în evidență primară – atribuirea identificatorului unic camerelor de corp ale Sistemului informațional;

5) asigurarea informațională – informația din Sistemul informațional este pusă la dispoziția autorităților publice, furnizorilor de date, destinatarilor și utilizatorilor în conformitate cu legislația;

9. Toate modificările în Sistemul informațional se păstrează în ordine cronologică.

10. Dreptul de acces la Sistemul informațional se realizează în funcție de roluri.

11. Sistemul informațional automatizat va fi găzduit pe platforma tehnologică guvernamentală comună (MCloud), iar dezvoltarea acestui sistem informațional va trebui să asigure integrarea bidirecțională cu sisteme informaționale partajate relevante (serviciul electronic guvernamental de autentificare și control al accesului (MPass), serviciul electronic guvernamental de jurnalizare (MLog) etc.).

12. Pentru formarea resursei informaționale, se asigură interacțiunea și schimbul de date cu următoarele resurse informaționale automatizate:

1) sistemul informațional automatizat de evidență a resurselor umane al Ministerului Afacerilor Interne;

2) serviciul electronic guvernamental integrat de semnătură electronică (MSign);

3) serviciul electronic guvernamental de jurnalizare (MLog);

4) serviciul electronic guvernamental de autentificare și control al accesului (MPass);

5) serviciul de notificare electronică (MNotify);

6) platforma de interoperabilitate (MConnect).

13. Sistemul informațional asigură exercitarea funcțiilor distincte determinate de destinația sa, grupate în contururi funcționale specifice, care sunt realizate prin intermediul software-ului aplicativ integrat de gestionare a înregistrărilor:

- 1) conturul funcțional „subdiviziunile subordonate ale utilizatorilor”:
 - a) evidența subdiviziunilor subordonate ale utilizatorilor;
 - b) evidența informației aferente fiecărei subdiviziuni subordonate ale utilizatorilor;
- 2) conturul funcțional „echipaj/patrula de serviciu”:
 - a) stabilirea și evidența echipajului/patrulei de serviciu conform evidențelor și asocierea acestora cu înregistrări și echipamente;
 - b) evidența informației aferente fiecărui echipaj/patrulă de serviciu;
- 3) conturul funcțional „înregistrare”:
 - a) formarea și evidența înregistrărilor video/audio;
 - b) formarea și evidența informației aferente fiecărei înregistrări;
 - c) transferul electronic al înregistrărilor către mediul de stocare;
- 4) conturul funcțional „utilizator”:
 - a) evidența utilizatorilor conform evidențelor efectuate de subdiviziunile subordonate ale utilizatorilor;
 - b) evidența informației aferente fiecărui utilizator și/sau utilizatorilor;
- 5) conturul funcțional „echipament”:
 - a) evidența echipamentelor de fixare/stocare video;
 - b) evidența informației aferente fiecărui echipament de fixare/stocare video;
 - c) anonimizarea datelor cu caracter personal.

Capitolul V

STRUCTURA ORGANIZATORICĂ A SISTEMULUI INFORMAȚIONAL

14. Proprietarul Sistemului informațional este statul.

15. Posesor al Sistemului informațional este Ministerul Afacerilor Interne, care asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional.

16. Deținător al Sistemului informațional este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, care exercită funcțiile de administrare tehnică, mentenanță și dezvoltare ale Sistemului informațional, în conformitate cu Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat și Hotărârea Guvernului nr. 317/2020 cu privire la organizarea și funcționarea Serviciului Tehnologii Informaționale. Acesta asigură gestionarea structurii infrastructurii MCloud, securitatea sistemului de infrastructură și infrastructura de comunicare.

17. Administratorul tehnic al Sistemului informațional este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică.

18. Utilizatorii Sistemului informațional sunt autoritățile administrative și instituțiile din subordinea Ministerului Afacerilor Interne: Inspectoratul General al

Poliției, Inspectoratul General al Poliției de Frontieră, Serviciul protecție internă și anticorupție, Inspectoratul General de Carabinieri, Inspectoratul General pentru Situații de Urgență și Biroul Migrație și Azil.

19. Modul și regulile de utilizare a echipamentelor ce fac parte din Sistemul informațional de supraveghere video portabil „Camera de corp”, de către funcționarii publici cu statut special/militar ai autorităților administrative și instituțiilor din subordinea Ministerului Afacerilor Interne, se stabilesc de ministrul afacerilor interne.

Capitolul VI

SPAȚIUL INFORMAȚIONAL AL SISTEMULUI INFORMAȚIONAL

Secțiunea 1

Obiectele informaționale ale Sistemului informațional

20. Obiectele informaționale specifice Sistemului informațional sunt:

- 1) camera de corp;
- 2) stația de andocare;
- 3) înregistrarea fixată;
- 4) utilizator (în situația când camera se transmite de la un utilizator la altul).

Secțiunea a 2-a

Identificatorii obiectelor informaționale

21. Fiecărui obiect informațional i se atribuie un identificator unic.

22. Identificator al obiectelor „cameră de corp”, „stația de andocare”, „înregistrarea fixată”, „utilizator”, este codul de referință (*numărul de ordine*) atribuit în cadrul Sistemului informațional.

Secțiunea a 3-a

Scenariile asociate obiectelor informaționale

23. Scenariile de bază reprezintă lista evenimentelor aferente obiectelor luate în evidența Sistemului informațional și corespund, în esență, celor ce urmează:

1) *luarea inițială în evidență*, care se face la apariția unui nou obiect al Sistemului informațional, cu atribuirea codului de referință de înregistrare corespunzător;

2) *actualizarea informației*, care se efectuează prin introducerea sistematică a modificărilor/rectificărilor/completărilor în baza de date a Sistemului informațional, în conformitate cu acțiunile întreprinse și/sau evenimentele survenite;

3) *scoaterea/radierea obiectului informațional* din evidență și transferarea datelor despre acesta în arhivă are loc prin efectuarea unei mențiuni speciale în baza de date.

Secțiunea a 4-a

Datele Sistemului informațional

24. Datele Sistemului informațional reprezintă totalitatea atributelor obiectului informațional și includ următoarele informații:

- 1) **pentru obiectul informațional „camera de corp”:**
 - a) informații despre utilizator;

- b) timpul de înregistrare continuă;
- c) timpul de pre – și post – înregistrare;
- d) numărul de înregistrare/identificatorul per dispozitiv;
- e) număr de serie;
- f) IMEI;
- g) număr de serie baterie;
- h) parolă per dispozitiv;
- i) rezoluție;
- j) unghi de vizualizare;
- k) termenul de păstrare a înregistrărilor;
- l) datele geospațiale;
- m) data înregistrării;
- n) conținutul înregistrărilor.

2) pentru obiectul informațional „stația de andocare”:

- a) informații despre deținător;
- b) numărul de înregistrare a stației de andocare;
- c) memorie operativă;
- d) spațiul de stocare incorporat;
- e) viteza de descărcare a informației;
- f) interfețe;
- g) indicatoare led: stare înregistrare, stare spațiul de stocare, stare conexiune

rețea, stare alimentare.

3) pentru obiectul informațional „înregistrare fixată”:

- a) data și ora înregistrării fixate;
- b) numărul de ordine al înregistrării fixate;
- c) lungimea/mărimea înregistrării fixate;
- d) datele geospațiale;
- e) parola de acces;
- f) viteza de descărcare a informației;

4) pentru obiectul informațional „utilizator”:

- a) nume, prenume, patronimic, IDNP-ului angajatului care utilizează camera;
- b) funcția;
- c) echipajul/patrula de serviciu;
- d) numărul de identificare al camerei de corp cu care a fost echipat.

Capitolul VII

SPAȚIUL TEHNOLOGIC

25. Sistemul informațional este proiectat ca un sistem modular, care asigură posibilitatea dezvoltării sale fără a afecta continuitatea funcționării. Arhitectura acestuia este concepută după schema-tip a infrastructurii informaționale a Sistemului informațional automatizat, în conformitate cu cerințele legale.

26. La nivel conceptual, arhitectura Sistemului informațional este definită pe 4 niveluri:

1) nivelul de interfață – serverul pentru paginile web cu formularele utilizatorilor și informațiile din baza de date pentru vizualizare și utilizare prin intermediul browser-ului stației de lucru;

2) produsul program al nivelului de mijloc – serverul aplicațiilor ce deservește interfața bazei de date cu utilizatorii, va transforma cererile utilizatorilor în interpelări SQL (un standard în domeniu, fiind cel mai popular limbaj utilizat pentru crearea, modificarea, regăsirea și manipularea datelor de către Sistemele de gestiune a bazelor de date relaționale), va primi datele de la baza de date și le va prezenta în formă comodă pentru percepție;

3) nivelul de transport – serverul care asigură interacțiunea cu stațiile de andocare și susțin procesele de deservire a activităților de copiere și transport date de la stațiile de andocare către serverul de stocare, formează bază de date stocate, realizează verificarea integrității și plenitudinii datelor recepționate/stocate de la stațiile de andocare către serverul de stocare;

4) nivelul de jos – serverul bazei de date.

27. Componenta centrală a infrastructurii Sistemului informațional este găzduită de către administratorul tehnic, în comun cu deținătorul, care asigură procesarea și stocarea centralizată a datelor aferente Sistemului informațional. Componentele distribuite reprezintă punctele de acces către componenta centrală prin canale securizate, asigurate de către deținător, de comun cu administratorul tehnic.

28. Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale, se determină la etapele inițiale și ulterioare de elaborare și implementare a Sistemului informațional de posesor și deținător, în colaborare cu elaboratorul de software, contractat conform procedurii legale de achiziționare a bunurilor/serviciilor.

29. Pentru comunicarea dintre nivelurile Sistemului informațional se utilizează rețelele de comunicații electronice ale Ministerului Afacerilor Interne al Republicii Moldova. Rețeaua de comunicații electronice a Sistemului informațional este definitivată de către elaboratorul de software, în colaborare cu deținătorul și posesorul Sistemului informațional.

30. Platforma tehnologică:

1) asigură formate unice de prezentare a datelor și protocoale comune de schimb de date;

2) oferă mecanisme de asigurare a concordanței bazelor de date ale Sistemului informațional cu cele ale sistemelor informaționale ale altor autorități publice. Concordanța este respectată în termeni de clasificatoare, nomenclatoare, completitudine etc.;

3) asigură un cadru formal și metodologic propice creării și implementării sistemului de management al securității informaționale.

31. Produsele program și echipamentele Sistemului informațional satisfac următoarele cerințe:

1) asigură posibilitatea stocării unor volume mari de informații;

2) asigură posibilitatea extinderii funcționale și a puterii de calcul (extensibilitate și scalabilitate);

- 3) susțin prelucrarea distribuită a datelor, accesul la resurse, atât în rețeaua locală, cât și în Internet;
- 4) utilizează un sistem unic de clasificare și codare (unificare);
- 5) funcționează pe diferite platforme hardware;
- 6) asigură fiabilitate înaltă;
- 7) asigură consistența și completitudinea informației;
- 8) susțin posibilitatea de modernizare în timpul procesului de exploatare.

32. Deținătorul, de comun cu Administratorul tehnic al Sistemului informațional, asigură găzduirea acestuia pe platforma tehnologică guvernamentală comună (MCloud).

Capitolul VIII

ASIGURAREA SECURITĂȚII INFORMAȚIONALE ȘI PROTECȚIA INFORMAȚIEI

33. Securitatea informațională presupune protecția Sistemului informațional, la toate etapele proceselor de creare, procesare, stocare și transmitere a datelor, de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea prejudiciului subiecților resurselor informaționale și infrastructurii informaționale.

34. Asigurarea securității informației este realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017 și Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123/2010. Pentru gestiunea riscurilor de securitate, posesorul, de comun cu deținătorul, elaborează și aprobă o politică generală de securitate. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate, pentru a verifica politica și conformitatea cu regulile de securitate, precum și, pentru a stabili domeniile care necesită îmbunătățiri.

35. Personalul implicat în utilizarea și administrarea Sistemului informațional este instruit în ceea ce privește riscurile de securitate la care poate fi expus.

36. Pericolele securității informaționale sunt:

- 1) colectarea și utilizarea ilegală a datelor;
- 2) încălcarea tehnologiei de prelucrare a datelor;
- 3) implementarea în produsele software și hardware a componentelor care îndeplinesc funcții neprevăzute în documentația aferentă;
- 4) elaborarea și răspândirea programelor ce afectează funcționarea normală a sistemelor informaționale și de telecomunicații, precum și a sistemelor securității informaționale;
- 5) nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor și sistemelor de prelucrare a datelor, de telecomunicații și comunicații;
- 6) influențarea sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor;
- 7) compromiterea cheilor și mijloacelor de protecție criptografică a

informației;

- 8) scurgerea informației prin canale tehnice;
- 9) implementarea dispozitivelor electronice pentru interceptarea informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor, utilizând sistemele de comunicații, precum și în încăperile de serviciu;
- 10) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;
- 11) interceptarea datelor în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și impunerea unei informații false;
- 12) utilizarea tehnologiilor informaționale naționale și internaționale necertificate, a mijloacelor de protecție a informației, a mijloacelor de informatizare, de telecomunicații și comunicații la crearea și dezvoltarea infrastructurii informaționale de telecomunicații;
- 13) accesul nesanționat la resursele informaționale din băncile și bazele de date;
- 14) încălcarea restricțiilor legale privind răspândirea informației;
- 15) încălcarea prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.

37. Sistemul asigură următoarele obiective de securitate:

- 1) autentificarea – garantează că informațiile cu accesibilitate limitată ale Sistemului informațional, sunt accesibile doar utilizatorilor de informație cu o identitate verificată prin serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- 2) autorizarea – garantează că utilizatorii de informație autentificați prin serviciul electronic guvernamental de autentificare și control al accesului (MPass) pot accesa serviciile și datele care corespund drepturilor lor de acces;
- 3) confidențialitatea – garantează că datele înregistrate în Sistemul informațional nu pot fi accesate de o parte terță neautorizată;
- 4) integritatea – garantează că datele înregistrate în Sistemul informațional nu au fost modificate sau alterate de o parte terță neautorizată.

38. În cadrul Sistemului informațional se aplică măsuri tehnice și organizatorice necesare pentru a asigura securitatea informațională, integritatea și confidențialitatea acestuia.

Capitolul XI

CONTROLUL ȘI RESPONSABILITATEA

39. Sistemul informațional este supus unui control intern și extern. Controlul intern este efectuat de subdiviziunile abilitate cu atribuții de control din cadrul posesorului/deținătorului Sistemului informațional, iar controlul extern este efectuat de către autoritățile/instituțiile publice investite cu acest drept.

40. Funcționalitatea eficientă și neîntreruptă a Sistemului informațional este asigurată de posesorul acestuia.

41. În funcție de rolul atribuit în Sistemul informațional, angajații Ministerului Afacerilor Interne poartă răspundere disciplinară, contravențională sau penală pentru

autenticitatea, fiabilitatea, integritatea datelor, precum și pentru păstrarea, stocarea și utilizarea informațiilor.

42. Funcționarea Sistemului informațional poate fi suspendată integral sau parțial, la solicitarea posesorului, a utilizatorilor, cu coordonarea posesorului sau la inițiativa deținătorului, cu informarea posesorului și utilizatorilor Sistemului informațional, în cazul apariției uneia dintre următoarele situații:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware ale Sistemului informațional;

2) la încălcarea cerințelor sistemului de securitate informațională;

3) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware ale Sistemului informațional.

43. În cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware ale Sistemului informațional din cauza terțelor persoane, este posibilă suspendarea funcționării Sistemului informațional, cu informarea subiecților prin mijloacele tehnice disponibile.

Anexa nr.2
la Hotărârea Guvernului
nr. din 2022

REGULAMENT
cu privire la organizarea și funcționarea Sistemului de supraveghere video
portabil „Camera de corp”

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul cu privire la organizarea și funcționarea Sistemului de supraveghere video portabil „Camera de corp” (în continuare – Regulament), stabilește procedurile și mecanismul de gestionare a camerelor de corp și a stațiilor de andocare de către angajații Ministerului Afacerilor Interne.

2. Scopul Regulamentului este stabilirea unui set unitar de reguli destinate implementării, gestionării, menținerii, suspendării și lichidării Sistemului informațional, precum și stabilirea cerințelor pentru angajații Ministerului Afacerilor Interne, în vederea accesării și utilizării înregistrărilor fixate de camerele de corp, respectând, în același timp obligațiile ce revin entității, în calitate de operator de date, conform Legii nr. 133/2011 privind protecția datelor cu caracter personal, precum și măsurile de securitate adoptate pentru protecția datelor cu caracter personal, protejarea vieții private, a intereselor legitime și garantarea drepturilor fundamentale ale persoanelor vizate.

3. Noțiunile utilizate în prezentul Regulament sunt corespunzătoare definițiilor de la pct. 2 al anexei nr. 1 la prezenta Hotărâre de Guvern.

4. Sistemul informațional este constituit din:

- 1) cameră de corp;
- 2) stație de andocare;
- 3) instrumentele software de gestiune, procesare și stocare centralizată a datelor.

5. Specificațiile tehnice ale camerei de corp și stației de andocare stabilite de specialiștii în domeniu, sunt aprobate de ministrul afacerilor interne.

6. Sistemul informațional se înregistrează în Registrul resurselor și sistemelor informaționale de stat.

7. Funcționarea Sistemului informațional este asigurată de către posesor până la adoptarea deciziei de lichidare a acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă, conform legislației.

Capitolul II
GESTIONAREA ȘI ASIGURAREA FUNCȚIONĂRII SISTEMULUI

8. Sistemul informațional se ține în formă automatizată.

9. Gestionarea Sistemului informațional în formă automatizată se realizează prin intermediul constituirii resursei informaționale, care reprezintă un ansamblu de obiecte informaționale.

10. Subiecții din domeniul creării, administrării, mentenanței, dezvoltării și utilizării Sistemului informațional:

- 1) Proprietarul Sistemului informațional este statul.
- 2) Posesorul Sistemului informațional este Ministerul Afacerilor Interne.
- 3) Deținător al Sistemului informațional este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne.
- 4) Administratorul tehnic al Sistemului informațional este Instituția publică Serviciul Tehnologii Informației și Securitate Cibernetică.
- 5) Utilizatorii Sistemului informațional sunt autoritățile administrative și instituțiile din subordinea Ministerului Afacerilor Interne (Inspectoratul General al Poliției, Inspectoratul General al Poliției de Frontieră, Serviciul protecție internă și anticorupție, Inspectoratul General de Carabinieri, Inspectoratul General pentru Situații de Urgență și Biroul Migrație și Azil) care asigură crearea resursei informaționale.

11. Introducerea datelor în Sistemul informațional se efectuează în baza înregistrărilor fixate de către camerele de corp.

12. Evidența obiectelor informaționale se ține în formă automatizată, conform prezentului Regulament.

13. Înregistrările fixate de camerele de corp se păstrează în Sistemul informațional în ordine cronologică, ceea ce asigură posibilitatea stocării informațiilor privind acțiunile desfășurate de angajații Ministerului Afacerilor Interne într-o etapă determinată de timp.

14. Termenul de păstrare a înregistrărilor în Sistemul informațional este de 180 zile, după care se radiază automat, în ordinea în care au fost stocate pe server. Păstrarea informațiilor se efectuează cu respectarea drepturilor și libertăților subiecților datelor cu caracter personal.

15. Termenul de stocare a înregistrărilor din Sistemul informațional poate fi prelungit în legătură cu:

- 1) actul procedural al agentului constatat, în legătură cu necesitatea folosirii acestora în calitate de probe în cazul unor eventuale contestații ale procesului-verbal cu privire la contravenție;
- 2) demersul motivat al organului de urmărire penală;
- 3) încheierea instanței judecătorești în legătură cu judecarea cauzei;
- 4) demersul motivat al subiecților care efectuează activitatea specială de investigații, în condițiile legii;
- 5) necesitatea examinării, gestionării și reacționării la incidentele de securitate produse în Sistemul informațional;
- 6) demersul motivat al autorităților administrative și instituțiilor din subordinea Ministerului Afacerilor Interne, în legătură cu desfășurarea anchetei de serviciu.

16. Termenul de stocare al înregistrărilor din Sistemul informațional nu poate fi prelungit decât pentru perioada necesară atingerii scopului urmărit, cu indicarea exactă a perioadei de timp.

17. Păstrarea Sistemului informațional este asigurată de deținător până la adoptarea deciziei despre lichidarea acestuia. În cazul lichidării Sistemului

informațional, datele și documentele conținute în acesta se transmit în arhivă conform legislației.

18. Pentru asigurarea funcționării eficiente și neîntrerupte a Sistemului informațional, schimbul informațional de date între subiecți este asigurat în regim non-stop.

19. Instruirea inițială a angajaților Ministerului Afacerilor Interne cu privire la gestionarea Sistemului informațional, utilizarea camerelor de corp, este realizată de angajator de comun cu reprezentanții companiei care livrează componentele acestuia.

Capitolul III

COMPETENȚA FUNCȚIONALĂ A POSESORULUI, DEȚINĂTORULUI ȘI ADMINISTRATORULUI TEHNIC

20. Posesorul are următoarele drepturi:

- 1) să elaboreze și să amendeze, în limitele competenței funcționale, cadrul normativ cu privire la Sistemul informațional;
- 2) să propună soluții de perfecționare și eficientizare a procesului de funcționare a Sistemului informațional, precum și să le pună în aplicare;
- 3) să supravegheze respectarea cerințelor de securitate a informației;
- 4) să solicite suspendarea/lichidarea Sistemului informațional.

21. Posesorul are următoarele atribuții:

- 1) asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional;
- 2) stabilește scopul și funcționalitățile Sistemului informațional în conformitate cu cadrul normativ relevant;
- 3) aprobă și coordonează cu administratorul tehnic, executarea modificărilor/rectificărilor solicitate în cererile privind erorile de sistem, erorile cauzate de factorul uman, incidentele de infrastructură care afectează funcționarea normală a Sistemului informațional;
- 4) asigură dezvoltarea continuă a Sistemului informațional prin adăugarea de noi componente;
- 5) exercită alte atribuții necesare asigurării bunei funcționări a Sistemului informațional.

22. Deținătorul este în drept să:

- 1) supravegheze respectarea cerințelor de securitate a informației;
- 2) acorde/revoce accesul la Sistemul informațional în cazurile de nerespectare a regulilor, standardelor și normelor în domeniul securității informaționale;
- 3) determine obiectele informaționale ale Sistemului informativ;
- 4) asigure măsurile tehnice și organizatorice de protecție și securitate;
- 5) ajusteze cerințele de securitate și conformitate ale Sistemului informativ la cerințele cadrului normativ în domeniul protecției datelor cu caracter personal;
- 6) gestionării utilizatorilor și angajaților din subordinea acestora, dar și accesul la sistem prin crearea, modificarea, eliminarea și setarea drepturilor acestora;

- 7) suspendării funcționării Sistemului, la solicitarea posesorului;
- 8) organizeze seminare și instruirii de utilizare a Sistemului informativ;
- 9) monitorizeze și supravegheze accesările informației și să identifice încălcările comise;
- 10) solicite suspendarea funcționării Sistemului.

23. Deținătorul are următoarele obligații:

- 1) asigură administrarea tehnică, mentenanța și dezvoltarea Sistemului informațional, precum și implementarea cerințelor de securitate stabilite de actele normative în domeniu;
- 2) să asigure funcționarea Sistemului informativ în conformitate cu regulile privind reglementarea resurselor informaționale;
- 3) să asigure implementarea măsurilor necesare pentru asigurarea regimului de confidențialitate și securitate a informației și a datelor cu caracter personal;
- 4) să garanteze utilizarea informației obținute din Sistemul informativ doar în scopurile stabilite de cadrul normativ;
- 5) să asigure securitatea sistemului de infrastructură și infrastructura de comunicare;
- 6) altele obligații stabilite în conformitate cu legislația.

24. Atribuțiile administratorului tehnic constau în asigurarea:

- 1) mentenanței Sistemului informațional;
- 2) accesului deplin securizat utilizatorilor și angajaților din subordinea acestora, la înregistrările și setările Sistemului informațional;
- 3) administrării tehnice, dar și a măsurilor tehnico-organizatorice pentru buna funcționare a Sistemului informațional;
- 4) după caz, a transportului securizat de date între camerele de corp și dispozitivele centrale de stocare și procesare a datelor Sistemului informațional, de comun cu deținătorul;
- 5) alocării spațiului pentru arhivarea înregistrărilor stocate pe server;
- 6) acordării suportului pentru dezvoltarea, implementarea și gestionarea Sistemului informațional;
- 7) implementării cerințelor de securitate stabilite de actele normative în domeniu;
- 8) funcționării Sistemului informativ în regim non-stop.

25. Atribuțiile utilizatorilor Sistemului informațional:

- 1) asigură evidența strictă, în format automatizat, asupra numărului și funcționării corespunzătoare a camerelor de corp, avute în gestiune, potrivit numărului de identificare;
- 2) desemnează prin act intern, lista nominală a angajaților care vor fi dotați cu camere de corp și lista angajaților responsabili de primirea/predarea camerelor de corp, care vor avea în același timp, dreptul de acces și furnizare a informației din Sistemul informațional, conform procedurii stabilite de legislație;
- 3) înaintează către deținător propuneri, privind actualizarea versiunii Sistemului informațional;

- 4) înaintează către deținător propuneri de dezvoltare a Sistemului informațional, în legătură cu inovațiile apărute în domeniul tehnologiilor informaționale;
- 5) asigură instruirea angajaților desemnați de a utiliza camerele de corp și a celor responsabili de accesarea informațiilor respective, în vederea asigurării securității informațiilor stocate în Sistemul informațional;
- 6) asigură prezentarea informațiilor din Sistemul informațional către solicitanții de informații, cu respectarea cadrului legal;
- 7) dispune de alte atribuții în conformitate cu legislația.

Capitolul IV

MODALITATEA DE GESTIONARE A CAMERELOR DE CORP

26. Camerele de corp și stațiile de andocare sunt repartizate de către posesor, autorităților administrative și instituțiilor din subordinea Ministerului Afacerilor Interne (utilizatori), configurate potrivit parametrilor tehnici ce asigură funcționalitatea deplină a întregului Sistem informațional.

27. Transmiterea camerelor de corp și a stațiilor de andocare către utilizatori se realizează prin ordinul ministrului afacerilor interne.

28. Camerele de corp și stațiile de andocare sunt stocate în spațiile special amenajate din cadrul subdiviziunilor utilizatorilor.

29. Utilizatorii desemnează lista nominală a angajaților din subordine din cadrul subdiviziunilor proprii, care vor utiliza camerele de corp și care vor avea acces la informația din Sistemul informațional, prin acte interne.

30. Fiecărei camere de corp îi este atribuit un număr de identificare.

31. Pentru o echipă alcătuită din cel puțin 2 angajați este prevăzută cel puțin o cameră de corp.

32. Transmiterea și primirea camerelor de corp către angajații din subordinea utilizatorilor se indică în Registrul de evidență al Sistemului de supraveghere video portabil „Camera de corp”, conform anexei nr.1 la Regulament.

33. Utilizarea camerelor de corp se efectuează în conformitate cu prevederile prezentului Regulament și a altor acte normative, exclusiv în timpul exercitării atribuțiilor de serviciu.

34. Utilizarea camerelor de corp se efectuează în mod vizibil și deschis, cu informarea obligatorie despre acest fapt de către angajații din subordinea utilizatorilor, a persoanelor și/sau străinilor cu care interacționează.

Prin excepție, informarea se poate realiza pe parcursul intervenției, în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale, în condițiile legii.

35. Camera de corp este atașată pe partea superioară a uniformei angajatului din subordinea utilizatorului, într-o poziție care asigură înregistrarea de înaltă calitate. Fiecare cameră de corp are atașat un indicator de avertizare, care informează despre înregistrarea evenimentelor.

36. Angajatul care utilizează camera de corp este obligat să pornească înregistrarea:

- 1) ținând cont de următorii factori:
 - a) securitatea și protecția personală;
 - b) necesitatea de a capta dovezi;
 - c) responsabilitate;
 - d) situații controversate;
 - e) implicarea persoanelor vulnerabile;
 - f) protecția persoanei și comunității;
 - g) orice alți factori obiectivi.
- 2) în următoarele cazuri:
 - a) la intervențiile în baza apelurilor de urgență;
 - b) investigării/documentării la fața locului a infracțiunilor, contravențiilor, incidentelor, inclusiv, în flagrant delict;
 - c) pentru înregistrarea locației obiectelor și urmelor de la fața locului sau în timpul unei situații de căutare la fața locului;
 - d) de la începutul și până la finalizarea efectuării măsurilor de constrângere;
 - e) în situații în care este posibilă aplicarea forței;
 - f) de la începutul și până la finalizarea efectuării perchezițiilor corporale;
 - g) de la începutul și până la finalizarea verificărilor și controalelor în încăperi;
 - h) când există o amenințare/pericol pentru viața și securitatea persoanelor și/sau a angajatului Ministerului Afacerilor Interne;
 - i) de la începutul și până la finalizarea protestelor/acțiunilor de dezordine în masă;
 - j) de la începutul și până la finalizarea acordării de suport persoanelor;
 - k) în cazurile în care conștientizarea înregistrării de către persoană, poate contribui la ameliorarea/rezolvarea eventualelor conflicte;
 - l) de la începutul și până la finalizarea conversațiilor cu persoanele care pot avea legătură cu un incident, sunt importante pentru o investigație, o eventuală procedură penală sau conțin informații posibil valoroase pentru justa soluționare a cazului;
 - m) de la începutul și până la finalizarea lichidării consecințelor situațiilor de urgență și/sau excepționale;
 - n) la necesitatea efectuării recunoașterii în timpul lichidării consecințelor situațiilor de urgență și/sau excepționale;
 - o) la indicația conducătorului ierarhic superior;
 - p) în scopul asigurării combaterii șederii ilegale a străinilor pe teritoriul Republicii Moldova și monitorizării fluxului de străini;
 - q) în alte cazuri, după necesitate.

37. În funcție de timpul zilei, înregistrarea se efectuează în modul „zi” sau „noapte”. Trecerea de la un regim la altul este automată.

38. La efectuarea înregistrării pe timp de noapte, zona de filmare este iluminată de către camera de corp, nefiind necesară iluminarea suplimentară a zonei respective.

39. După activarea/conectarea camerei de corp, toată comunicarea/interacțiunea angajatului este înregistrată în mod continuu.

40. Camera de corp nu este utilizată în următoarele circumstanțe:

- 1) pentru înregistrarea integrală a unei ture planificate, cu excepția cazului în care este justificat de circumstanțele specifice;
- 2) pentru înregistrarea materialelor care nu au legătură cu îndeplinirea atribuțiilor de serviciu;
- 3) la cel mult 25 de metri de un dispozitiv suspect sau de un material inflamabil.

41. Conectarea de la distanță a camerei de corp se efectuează:

- 1) în timpul efectuării măsurilor speciale de investigații;
- 2) când este apăsat butonul de alarmă de către angajatul Ministerului Afacerilor Interne.

42. Atribuțiile angajatului responsabil de primirea/predarea camerelor de corp:

- 1) ține evidența strictă, în format automatizat, asupra numărului și funcționării corespunzătoare a camerelor de corp, avute în gestiune, potrivit numărului de identificare;
- 2) asigură evidența predării, primirii și depozitării camerelor de corp de la/către angajații desemnați;
- 3) verifică funcționalitatea camerelor de corp la primirea acestora de la angajații desemnați, în prezența lor, ținând cont de următoarele aspecte:
 - a) starea contactelor;
 - b) corespunderea numărului de identificare;
 - c) mecanismul de fixare;
- 4) calitatea imaginii de pe ecranul camerei de corp, starea bateriei, corectitudinea orei și datei, asigurând efectuarea deconectării/conectării camerei de corp și, după caz, va asigura efectuarea unei poze sau a unei înregistrări video/audio;
- 5) în absența obiecțiilor cu privire la starea tehnică a camerei de corp primite, persoana responsabilă de primirea/predarea camerelor de corp, notează despre primirea acesteia în Registrul de evidență al Sistemului de supraveghere video portabil „Camera de corp” (anexa nr. 1 la Regulament) și plasează camera de corp în depozitul special;
- 6) în decurs de 3 ore de la primirea camerei de corp, persoana responsabilă de primirea/predarea camerelor de corp, efectuează procedura de stocare a înregistrărilor de pe camerele de corp către stația de andocare și, ulterior pe server, conform Instrucțiunilor de utilizare a stațiilor de andocare pentru camere de corp, aprobate de ministrul afacerilor interne, pregătind, astfel, camera de corp pentru următoarea utilizare;
- 7) în caz de depistare a deteriorării sau pierderii camerei de corp de către angajatul aflat în tură/serviciu, persoana responsabilă de primirea/predarea camerelor de corp informează imediat în scris conducătorul autorității administrative sau instituției din subordinea Ministerului Afacerilor din care face parte.
- 8) asigură vizualizarea, eliberarea înregistrărilor din Sistemul informațional, conform procedurii stabilite de legislație.

43. Atribuțiile angajatului dotat cu camera de corp:

- 1) utilizează camera de corp în vederea exercitării atribuțiilor funcționale;
- 2) inspectează și verifică în mod independent funcționalitatea camerei de corp, primită înainte de începerea turei/serviciului;
- 3) consemnează despre primirea camerei de corp în Registrul de evidență al Sistemului de supraveghere video portabil „Camera de corp” (anexa nr. 1 la Regulament), dacă aceasta este în stare de funcționare, nu prezintă defecțiuni externe și nu sunt careva obiecții;
- 4) menține lentila de la camera de corp în stare curată, pentru a asigura calitatea înregistrărilor;
- 5) predă camera de corp la sediul subdiviziunii utilizatorului, în cel mai scurt timp posibil după finalizarea serviciului/turei.

44. În cazul deteriorării camerei de corp sau a funcționării defectuoase a acesteia, angajatul dotat cu camera de corp este obligat să anunțe imediat conducătorul ierarhic superior, iar la predarea camerei de corp, întocmește un raport cu indicarea circumstanțelor în care aceasta a fost deteriorată.

45. Angajații desemnați să utilizeze camerele de corp sunt în drept:

- 1) să beneficieze de o pregătire generală pentru utilizarea eficientă a camerelor de corp și a stațiilor de andocare;
- 2) să li se ofere suportul metodologic și practic pentru utilizarea camerelor de corp, stațiilor de andocare sau alte părți componente ale Sistemului informațional (instrumente software de gestiune etc.);
- 3) să exercite și alte drepturi în conformitate cu legislația.

46. Angajații desemnați să utilizeze camerele de corp sunt obligați:

- 1) să urmeze cursurile de instruire privind utilizarea camerelor de corp și a stației de andocare;
- 2) să folosească cu atenție camera de corp și stația de andocare, doar în conformitate cu destinația acesteia;
- 3) să nu folosească camera de înregistrare în scopuri personale;
- 4) să respecte condițiile tehnice de utilizare a camerelor de corp și a stației de andocare;
- 5) să se abțină de la acțiunile/inacțiunile care ar putea duce la deteriorarea camerei de corp și/sau a stației de andocare;
- 6) să utilizeze înregistrările video/audio în conformitate cu Codul de procedură penală nr. 122/2003, Codul contravențional nr. 218/2008, Codul de procedură civilă nr. 225/2003, Codul administrativ nr. 116/2018, Legea nr. 982/2000 privind accesul la informație și Legea nr. 133/2011 privind protecția datelor cu caracter personal;
- 7) să asigure confidențialitatea și securitatea datelor cu caracter personal, în cadrul prelucrării înregistrărilor video/audio, potrivit legislației din domeniul protecției datelor prenotate.

Capitolul V

ASIGURAREA PROTECȚIEI DATELOR CU CARACTER PERSONAL DIN SISTEMUL INFORMAȚIONAL

Secțiunea 1

Securitatea informației Sistemului informațional

47. Sistemul informațional se conformează cerințelor minime de securitate corespunzătoare cerințelor de securitate a aplicațiilor livrate din platforma MCloud.

48. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul Sistemului informațional se efectuează cu respectarea 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 nr. 1123/2010.

49. Protecția informației cu caracter personal se efectuează prin următoarele metode:

1) prevenirea conexiunilor neautorizate la rețelele de transport de date și interceptării cu ajutorul mijloacelor tehnice specifice a datelor din Sistemul informațional transmise prin aceste rețele;

2) asigurarea măsurilor de protecție a datelor prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport de date;

3) excluderea accesului neautorizat la datele din Sistemul informațional prin utilizarea funcționalităților de autorizare ale serviciului MPass;

4) prevenirea acțiunilor speciale tehnice și de program care duc la distrugerea, denaturarea datelor sau cauzează defecțiuni în funcționarea complexului tehnic și de program;

5) efectuarea tuturor măsurilor aferente asigurării restabilirii și continuității funcționării Sistemului informațional în cazul incidentelor;

6) prevenirea acțiunilor intenționate și/sau neintenționate ale angajaților din subordinea utilizatorilor, care pot duce la distrugerea sau denaturarea datelor din Sistemul informațional.

50. În cazul incidentelor de securitate, administratorul tehnic va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate.

51. Prelucrarea de date în cadrul Sistemului informațional garantează respectarea următoarelor principii privind protecția datelor cu caracter personal:

1) specificarea și limitarea scopului;

2) adoptarea de măsuri tehnice și organizaționale în scopul asigurării unui nivel adecvat de protecție a datelor cu caracter personal, în conformitate cu legislația.

52. Accesul pentru vizualizarea sau efectuarea copiilor ale înregistrărilor stocate pe server este limitat și permis reprezentanților organelor de drept doar în baza unui demers motivat.

53. Persoanele care au avut acces la vizualizarea sau obținerea copiilor înregistrărilor stocate pe server, se indică în Registrul de evidență al accesărilor la înregistrările stocate în Sistemul de supraveghere video portabil „Camera de corp”, conform anexei nr. 2 la prezentul Regulament.

54. Accesarea informației din Sistemul informațional se va realiza în baza unui motiv întemeiat legal (existența unei solicitări oficiale, cereri, plângeri, dosar contravențional/penal etc.), prin care s-ar demonstra legătura de cauzalitate directă dintre datele cu caracter personal prelucrate și necesitatea accesării acestora, cu

condiția prelucrării unui volum de date neexcesiv, stric necesar în ceea ce privește atingerea scopului propus.

55. Deținătorul sau utilizatorul Sistemului informațional va asigura furnizarea informației în termenele prevăzute de legislație.

Secțiunea a 2-a

Folosirea înregistrărilor de pe camera de corp și accesarea acestora

56. Utilizarea înregistrărilor de pe cameră de corp, stația de andocare sau server se materializează prin actul de reproducere, copiere, distribuire, publicare, traducere, difuzare la televiziune, difuzare pe rețeaua Internet, editare și utilizare a conținutului înregistrării în orice alt mod prevăzut de legislație.

57. Înregistrările fixate de camerele de corp:

1) pot fi furnizate angajaților Ministerului Afacerilor Interne, instanțelor judecătorești, precum și organului de urmărire penală în cadrul procedurilor penale, cu scopul de a-și îndeplini sarcinile, atribuțiile de serviciu, în baza unor solicitări oficiale;

2) pot fi transmise pentru utilizare reprezentanților mass-media și, în cazuri excepționale, pot fi distribuite pe Internet, exclusiv pentru prevenirea faptelor ilegale și asigurarea securității naționale, protecției persoanei, societății și statului, cu condiția că interesul public predomină interesului personal al persoanei vizate în înregistrare, în acest caz:

a) imaginea persoanelor este blurată;

b) eliberarea oricărui material destinat vizualizării publice este efectuată conform procedurii legale stabilite.

3) în cazul pornirii procesului penal sau contravențional, furnizarea înregistrărilor să efectuează cu respectarea prevederilor Codului de procedură penală nr. 122/2003, Codului contravențional nr. 218/2008 și a legislației privind protecția datelor cu caracter personal.

Capitolul VI

CONTROLUL ȘI RĂSPUNDEREA

58. Sistemul informațional este supus unui control intern și extern.

59. Controlul intern este efectuat de către subdiviziunile abilitate cu atribuții de control pe domeniul ce face obiectul de reglementare a prezentului Regulament ale posesorului sau deținătorului, iar cel extern – de către instituțiile abilitate și certificate în domeniul tehnologiei informației.

60. Subdiviziunile cu atribuții de control ale utilizatorilor verifică trimestrial Registrul de evidență al accesărilor la înregistrările stocate în Sistemul informațional, în vederea stabilirii corectitudinii completării acestuia și verificării temeiniciei scopului declarat la accesarea datelor stocate din Sistemul menționat.

61. Controlul legalității operațiunilor de prelucrare a datelor cu caracter personal se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter Personal.

62. La efectuarea controlului extern, organul de control alcătuiește un act privind controlul extern efectuat (act, raport, proces-verbal, prescripție, etc).

Posesorul, după caz, utilizatorul este obligat să ia măsuri pentru lichidarea încălcărilor identificate și să informeze despre aceasta organul de control.

63. Pentru organizarea controlului de funcționare al Sistemului informațional este responsabil utilizatorul sau, după caz, deținătorul care este obligat să asigure dreptul de acces la mijloacele de ținere a acestuia, respectiv în încăperile în care se află mijloacele hardware.

64. Angajații subiecților Sistemului informațional poartă răspundere în conformitate cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal, pentru autenticitatea, fiabilitatea, integritatea informației, precum și pentru păstrarea/stocarea și utilizarea acesteia.

65. Destinatarii informațiilor ce conțin date cu caracter personal poartă răspundere pentru prelucrarea neconformă a datelor cu caracter personal, potrivit prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.

66. Pentru nerespectarea prevederilor prezentului Regulament, subiecții Sistemului informațional poartă răspundere în conformitate cu legislația.

Anexa nr.1
la Regulamentul cu privire la organizarea și
funcționarea sistemului de supraveghere
video portabil „Camera de corp”

REGISTRUL DE EVIDENȚĂ
a camerelor de corp ale
Sistemului informațional de supraveghere video portabil
„Camera de corp”

Nr.	Nume, prenume, patronimic	Funcția	Echipajul /Patrula	Nr. de identificare al camerei	Ziua, luna, anul, ora primirii	Semnătura	Ziua, luna, anul, ora predării	Semnătura
1								
2								

Anexa nr.2
la Regulamentul cu privire la organizarea și
funcționarea sistemului de supraveghere
video portabil „Camera de corp”

REGISTRUL DE EVIDENȚĂ
al accesării înregistrărilor stocate în Sistemul
de supraveghere video portabil
„Camera de corp”

Nr.	Ziua, luna, anul accesării	N.P.P/funcția persoanei care solicită accesul/efectuarea copiei	Tipul accesării (vizualizare/ efectuarea copiei)	Temeiul accesării	N.P.P angajatului care a accesat înregistrarea	Semnătură	
						Persoana care a accesat înregistrarea	Persoana care a solicitat accesul/ efectuarea copiei
1.							
2.							