

Aprobată

prin Ordinul nr. 683 din 13.07.2026

Secretar General al FMF,

Butelschi Serghei

**POLITICA DE SECURITATE
PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL
LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR INFORMAȚIONALE
GESTIONATE DE FEDERAȚIA MOLDOVENEASCĂ DE FOTBAL**



I. DISPOZIȚII GENERALE

1. Prin prezentul act, Federația Moldovenească de Fotbal (în continuare – "FMF") informează subiecții vizați despre politica de securitate adoptată în cadrul instituției și aplicată de angajații FMF în cadrul realizării activităților de prelucrare a datelor cu caracter personal.
2. Prin prezentul act, FMF declară că asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și asigură dreptul la inviolabilitatea vieții private.
3. Prin prezentul act, FMF confirmă că la prelucrarea datelor cu caracter personal în cadrul instituției sunt aplicate principiile prevăzute de Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal (până la data abrogării – 23 august 2026) și Legea nr. 195 din 25 iulie 2024 privind protecția datelor cu caracter personal (începând cu data intrării în vigoare – 23 august 2026).
4. Prezenta Politică de Securitate reprezintă un document care informează subiecții de date despre activitățile de prelucrare realizate în cadrul FMF, scopurile acestora, precum și măsurile de securitate aplicate de FMF în contextul activităților de prelucrare realizate, ținându-se cont de potențiale pericole și riscuri reale la care pot fi expuse datele cu caracter personal ale subiecților vizați.
5. În prezenta Politică de Securitate, sunt utilizate următoarele noțiuni și acestea vor fi interpretate după cum urmează:
 - a) **date cu caracter personal** – orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;
 - b) **categorii speciale de date cu caracter personal** – datele care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, apartenența la sindicate, precum și prelucrarea datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea sau a datelor privind viața sexuală ori orientarea sexuală ale unei persoane fizice, precum și cele privind condamnările penale ale unei persoane fizice.

- c) **operator** – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;
- d) **persoană împuternicită de către operator** – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator;
- e) **autentificare** – verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;
- f) **control de securitate** – acțiuni întreprinse în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;
- g) **fișiere temporare** – ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat pînă la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;
- h) **identificare** – atribuirea unui identificator subiecților și obiectelor de acces și/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;
- i) **integritate** – certitudinea, necontradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;
- j) **mijloace de protecție criptografică a informației care conține date cu caracter personal** – mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicații;
- k) **nivel de protecție** – nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor, elaborat și actualizat corespunzător nivelului dezvoltării tehnologice și costurilor implementării acestor măsuri;
- l) **politica de securitate a datelor cu caracter personal** – document, elaborat de către operatorul de date care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru securitatea datelor, ținîndu-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sunt expuse acestea;
- m) **perimetru de securitate** – zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic și/sau tehnic al accesului;
- n) **persoana responsabilă de politica de securitate a datelor cu caracter personal** – persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;
- o) **protecția informației contra acțiunilor neintenționate** – ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține date cu caracter personal;
- p) **purtător de date cu caracter personal** – suport magnetic, optic, laser, de hîrtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;

- q) **restaurarea datelor** – procedurile cu privire la reconstituirea/restabilirea datelor cu caracter personal în starea în care se aflau până la momentul pierderii sau distrugerii acestora;
- r) **tehnologie informațională** – totalitatea metodelor, procedeelor și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;
- s) **utilizator** – persoana care acționează sub autoritatea deținătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal;
- t) **sesiune de lucru** – perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și până la momentul opririi acestora;
- u) **sistem informațional de date cu caracter personal** – totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal;
- v) **prelucrarea datelor cu caracter personal** – orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;
- w) **stocare** – păstrarea pe orice fel de suport a datelor cu caracter personal;
- x) **sistem de evidență a datelor cu caracter personal** – orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice;
- y) **consimțământul subiectului datelor cu caracter personal** – orice manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;
- z) **depersonalizarea datelor** – modificarea datelor cu caracter personal astfel încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă.

II. OBIECTIVELE POLITICII DE SECURITATE

6. Obiectivele principale ale Politicii sunt legate de asigurarea disponibilității, integrității și confidențialității tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de FMF, atât în cadrul prelucrării manuale, cât și în cadrul prelucrării automate.

7. Asigurarea securității informaționale reprezintă o componentă esențială a activității FMF, aceasta fiind orientată atât asupra asigurării securității mediului fizic, cât și asupra tehnologiilor și sistemelor informaționale utilizate, cât și asupra utilizării bunelor practici în contextul activităților de prelucrare de date.

8. Având în vedere că siguranța tehnologiilor informaționale și a comunicației nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic și de altă natură.

9. FMF va asigura protecția datelor cu caracter personal atât ale angajaților săi, cât și ale clienților și altor categorii de beneficiari.

10. Prezentul document nu constituie parte componentă a contractului individual de muncă sau a contractului comercial, dar reprezintă o condiție a activității de muncă și/sau de activitate comercială în cadrul FMF. Pornind de la această reglementare, toți angajații, clienții și alți beneficiari ai serviciilor oferite de către FMF urmează să respecte strict prevederile Politicii și ale regulamentelor interne ale FMF privind protecția datelor cu caracter personal prelucrate în cadrul acesteia. Orice încălcare a prevederilor prezentei Politici va genera răspunderea juridică a persoanei în cauză.

III. PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

11. Orice prelucrare de date cu caracter personal în cadrul FMF trebuie să fie realizată cu respectarea următoarelor principii:

11.1. prelucrarea urmează a fi realizată în mod corect și în conformitate cu prevederile legale;

11.2. colectarea urmează a fi realizată în scopuri determinate, explicite și legitime, iar ulterior să nu fie admisă prelucrarea într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau științifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor legale, inclusiv privind notificarea către Centrul Național pentru Protecția Datelor cu Caracter Personal, și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică și cea științifică;

11.3. asigurarea colectării unor date adecvate, pertinente și neexcesive în ceea ce privește scopul pentru care sunt colectate și/sau prelucrate ulterior;

11.4. asigurarea colectării unor date exacte și, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate și ulterior prelucrate se șterg sau se rectifică;

11.5. stocarea într-o formă care să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sunt colectate și ulterior prelucrate. Stocarea datelor cu caracter personal pe o perioadă mai mare, în scopuri statistice, de cercetare istorică sau științifică, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează aceste domenii, și numai pentru perioada necesară realizării acestor scopuri.

IV. COLECTAREA DATELOR CU CARACTER PERSONAL. NOMENCLATORUL DATELOR CU CARACTER PERSONAL

12. În cadrul FMF, colectarea și prelucrarea datelor cu caracter personal se realizează în următoarele scopuri, corespunzătoare activităților efectiv desfășurate de FMF:

12.1. legitimarea, evidența și transferul jucătorilor, antrenorilor și oficialilor de club, precum și administrarea registrelor și bazelor de date sportive gestionate de FMF (sistemul de legitimări și transferuri, evidența membrilor afiliați);

12.2. organizarea și desfășurarea competițiilor sportive naționale, inclusiv evidența participanților, a rezultatelor sportive și a arbitrilor/oficialilor delegați;

12.3. organizarea și administrarea activității selecționatelor naționale (toate categoriile de vârstă), inclusiv convocarea, evidența și deplasarea loturilor reprezentative;

- 12.4.** licențierea cluburilor de fotbal și acreditarea agenților sportivi (intermediarilor), în conformitate cu regulamentele FMF și ale forurilor fotbalistice internaționale (FIFA, UEFA);
- 12.5.** activitatea organelor disciplinare și de etică ale FMF, inclusiv investigarea și soluționarea abaterilor disciplinare, contestațiilor și litigiilor sportive;
- 12.6.** prevenirea și combaterea manipulării competițiilor sportive (fraudei/pariurilor ilegale) și asigurarea integrității competiționale, inclusiv prin cooperarea cu autoritățile competente și forurile fotbalistice internaționale;
- 12.7.** controlul medico-sportiv și antidoping al jucătorilor legitimați și al membrilor loturilor reprezentative, inclusiv evidența certificatelor medicale de aptitudine sportivă și a accidentărilor;
- 12.8.** prelucrarea datelor cu caracter personal ale minorilor legitimați sau participanți la programele de selecție/pregătire ale FMF, în condițiile speciale prevăzute la Cap. V;
- 12.9.** acreditarea și evidența arbitrilor, observatorilor, oficialilor de meci și a personalului tehnic delegat la competiții;
- 12.10.** organizarea cursurilor de licențiere și formare profesională a antrenorilor și a altor categorii de personal tehnic din fotbal, a altor specialiști conform programelor din cadrul Academiei FMF;
- 12.11.** asigurarea securității spectatorilor și a ordinii publice la evenimentele sportive, inclusiv prin sisteme de control al accesului, acreditare și, după caz, video-supraveghere la stadioane și centrele de pregătire, de asemenea, în oficii, magazine și depozite;
- 12.12.** evidența comercială a partenerilor, sponsorilor și clienților FMF, inclusiv gestionarea contractelor comerciale, de sponsorizare și de drepturi media;
- 12.13.** evidența și registrul angajaților FMF, gestionarea dosarelor personale, administrarea raporturilor de muncă, calcularea și achitarea drepturilor salariale și respectarea obligațiilor legale în domeniul resurselor umane;
- 12.14.** recrutarea și selecția personalului administrativ și tehnic al FMF;
- 12.15.** evidența și prelucrarea contabilă, inclusiv raportarea datelor financiar-contabile către autoritățile competente, în conformitate cu legislația în vigoare;
- 12.16.** asigurarea securității persoanelor, bunurilor și patrimoniului FMF, inclusiv prin utilizarea sistemelor de supraveghere video în oficii, magazine, centrele de pregătire a selecționatei și spațiile de depozitare a echipamentului sportiv;
- 12.17.** controlul accesului în incintele FMF și evidența timpului de muncă a personalului angajat, în scopul asigurării disciplinei muncii și securității spațiilor;
- 12.18.** gestionarea reclamațiilor, cererilor și solicitărilor adresate FMF, în scopul soluționării acestora și protejării intereselor legitime ale FMF;
- 12.19.** administrarea sistemelor IT și a conturilor de utilizator, în scopul funcționării corespunzătoare și securității sistemelor informatice;
- 12.20.** prevenirea, identificarea, investigarea și raportarea incidentelor de securitate a datelor cu caracter personal și a informațiilor;
- 12.21.** administrarea website-ului și a platformelor online ale FMF, inclusiv comunicarea cu utilizatorii, difuzarea rezultatelor sportive și furnizarea serviciilor online;
- 12.22.** desfășurarea activităților de marketing, comunicare și promovare a fotbalului moldovenesc, inclusiv gestionarea imaginii jucătorilor și oficialilor în materiale oficiale FMF, cu respectarea, în cazul minorilor, a regimului special prevăzut la Cap. V;
- 12.23.** analiza traficului web și realizarea de statistici (cookies, analytics), în scopul îmbunătățirii serviciilor și experienței utilizatorilor;
- 12.24.** investigarea incidentelor interne disciplinare sau patrimoniale, în scopul protejării patrimoniului FMF și exercitării drepturilor legale ale angajatorului;

12.25. gestionarea litigiilor și a procedurilor judiciare, administrative sau sportive (inclusiv în fața Curții de Arbitraj Sportiv/TAS), în scopul apărării drepturilor și intereselor legitime ale FMF;
12.26. arhivarea documentelor de personal, contabile, comerciale, medicale și sportive, în conformitate cu obligațiile legale și regulamentare de păstrare și arhivare;
12.27. transferul datelor cu caracter personal ale jucătorilor, oficialilor și angajaților către forurile fotbalistice internaționale (FIFA, UEFA) și către parteneri externi sau furnizori de servicii, în scopul organizării deplasărilor de serviciu peste hotare, participării la competiții internaționale, vizite de lucru, instruiți, conferințe sau alte evenimente profesionale.

13. În acest sens vor fi colectate date cu caracter personal, care direct sau indirect identifică o persoană fizică, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale. Datele cu caracter personal se împart în două categorii: obișnuite și speciale.

14. Din categoria specială a datelor cu caracter personal, FMF **nu colectează** date privind originea rasială sau etnică, opiniile politice, confesiunea religioasă, convingerile filozofice, apartenența la sindicate sau condamnările penale. FMF **colectează și prelucrează**, exclusiv în scopurile strict necesare activității sportive (controlul medico-sportiv, antidoping, asigurarea capacității de joc, măsuri de securitate la evenimente sportive), date privind sănătatea și, după caz, date biometrice, cu respectarea temeiurilor legale prevăzute la art. 9 din Legea nr. 195/2024 (consimțământ explicit, interes public substanțial în domeniul sportului sau motive de medicină a muncii) și cu aplicarea unor măsuri de securitate sporite.

15. Din **categoria obișnuită a datelor** cu caracter personal va fi colectată informația care dezvăluie:

- 15.1.** numele, prenumele;
- 15.2.** sexul;
- 15.3.** data și locul nașterii;
- 15.4.** cetățenia;
- 15.5.** IDNP;
- 15.6.** imagine;
- 15.7.** situația familială;
- 15.8.** situația militară;
- 15.9.** datele personale ale membrilor de familie;
- 15.10.** datele din permisul de conducere;
- 15.11.** situația economică și financiară;
- 15.12.** datele bancare;
- 15.13.** semnătura;
- 15.14.** datele din actele de stare civilă;
- 15.15.** numărul dosarului de pensie;
- 15.16.** codul personal de asigurării sociale (CPAS);
- 15.17.** codul asigurării medicale (CPAM);
- 15.18.** numărul de telefon/fax;
- 15.19.** numărul de telefon mobil;
- 15.20.** adresa (domiciliului/reședinței);
- 15.21.** adresa e-mail;
- 15.22.** profesia și/sau locul de muncă;
- 15.23.** formarea profesională – diplome – studii;
- 15.24.** obiceiurile/ preferințele/ comportamentul.

V. PRELUCRAREA DATELOR CU CARACTER PERSONAL ALE MINORILOR

16. În sensul prezentei Politici, este considerat minor subiectul de date cu caracter personal care nu a împlinit vârsta de 18 ani, inclusiv copiii legitimați la cluburile afiliate FMF, participanții la selecționatele naționale de juniori (toate categoriile de vârstă) și participanții la programele de pregătire, selecție sau detectare a tinerelor talente organizate sau supravegheate de FMF.

17. Prelucrarea datelor cu caracter personal ale minorilor se realizează cu respectarea unui nivel sporit de protecție, ținând cont de vulnerabilitatea acestei categorii de subiecți de date, în conformitate cu principiile generale privind protecția datelor copiilor prevăzute de Legea nr. 195 din 25 iulie 2024 privind protecția datelor cu caracter personal (în vigoare din 23 august 2026) și, până la acea dată, de Legea nr. 133/2011.

18. Categoriile de date cu caracter personal ale minorilor colectate de FMF, exclusiv în scopul organizării activității sportive (legitimare, participare la competiții, evidență medico-sportivă, comunicare oficială a rezultatelor), sunt:

- a)** datele de identificare prevăzute la pct. 15.1–15.6, 15.20–15.21;
- b)** datele privind reprezentantul legal (nume, prenume, date de contact) necesare pentru obținerea consimțământului și comunicarea oficială;
- c)** certificatul medical de aptitudine sportivă și alte date privind sănătatea strict necesare confirmării capacității de joc, colectate în condițiile pct. 14;
- d)** imaginea minorului, rezultată din activitatea sportivă oficială (fotografii/înregistrări din cadrul competițiilor, cantonamentelor sau evenimentelor oficiale ale FMF).

19. Consimțământul reprezentantului legal

- a)** prelucrarea datelor cu caracter personal ale minorului se realizează în baza consimțământului scris, expres și prealabil al reprezentantului legal (părinte sau tutore), obținut înainte de legitimare, înscrierea la competiții sau participarea la orice program organizat de FMF;
- b)** consimțământul este solicitat separat pentru fiecare scop distinct de prelucrare (participare sportivă, evidență medicală, comunicare/publicare a imaginii), fiind interzisă condiționarea participării sportive a minorului de acordarea consimțământului pentru scopuri neesențiale (spre exemplu, promovare comercială sau marketing);
- c)** reprezentantul legal are dreptul de a-și retrage consimțământul în orice moment, printr-o cerere scrisă adresată FMF sau clubului afiliat, retragerea neafectând legalitatea prelucrării efectuate anterior;
- d)** FMF pune la dispoziția reprezentantului legal informații privind prelucrarea datelor minorului, redactate într-un limbaj clar și accesibil, iar la cererea reprezentantului legal, informații adaptate vârstei și gradului de înțelegere al minorului.

20. Limitarea comunicării publice a imaginii minorilor

- a)** publicarea imaginii minorilor (fotografii, materiale video, liste nominale) pe canalele de comunicare ale FMF (website, rețele sociale, materiale de presă) se realizează exclusiv cu consimțământul prealabil al reprezentantului legal, obținut odată cu acordul pentru participarea sportivă;

b) este interzisă publicarea, alături de imaginea minorului, a unor date suplimentare care ar permite identificarea sau localizarea acestuia în afara contextului sportiv oficial (adresa de domiciliu, unitatea de învățământ, rutine zilnice, date de contact personale);

c) FMF nu va utiliza imaginea minorilor în scopuri comerciale sau publicitare care depășesc promovarea activității sportive oficiale, fără un consimțământ distinct și expres al reprezentantului legal pentru acest scop specific;

d) reprezentantul legal poate solicita oricând, printr-o cerere scrisă, retragerea unei imagini a minorului de pe canalele oficiale ale FMF, cerere care va fi soluționată în cel mai scurt termen rezonabil;

e) este interzisă transmiterea sau dezvăluirea imaginii ori a altor date ale minorilor către terți neafiliați scopului sportiv oficial (agenți, sponsori, parteneri media), în afara cazurilor expres autorizate de reprezentantul legal.

21. Persoanele din cadrul FMF care au acces la datele minorilor (antrenori, personal medical, administratori ai bazelor de date) sunt instruite în mod distinct cu privire la regimul special de protecție aplicabil acestei categorii de subiecți de date, instruirea fiind consemnată conform prezentei Politici.

22. Datele cu caracter personal ale minorilor se păstrează doar pe durata necesară scopului pentru care au fost colectate (participare la categoria de vârstă respectivă, evidență istorică a palmaresului sportiv), fiind șterse sau anonimizate la încetarea acestui scop, cu excepția cazurilor în care legislația impune o perioadă de arhivare mai mare.

VI. DISPOZIȚII PRIVIND PERSOANA RESPONSABILĂ DE POLITICA DE SECURITATE

23. Operatorul de date cu caracter personal (FMF), ținând cont de specificul activității, prin prezenta Politică de securitate, transpune procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență gestionate.

24. Politica de securitate a datelor cu caracter personal se va revizui cel puțin o dată pe an ca rezultat al modificărilor sau reevaluării activităților FMF, responsabilă de ajustarea prevederilor prezentului act fiind desemnată persoana responsabilă de implementarea și monitorizarea respectării prevederilor prezentului document.

25. Politica de securitate, în mod obligatoriu, va fi adusă la cunoștință, sub semnătură, tuturor angajaților responsabili de prelucrarea datelor cu caracter personal, înainte acordării accesului la prelucrarea datelor cu caracter personal, inclusiv la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecție a datelor cu caracter personal.

26. Responsabil de implementarea și monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal este desemnată persoana care, conform fișei postului și/sau ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament și buget) și va avea acces liber la informația necesară pentru îndeplinirea funcțiilor sale, în măsura în care aceasta nu operează în afara cadrului acestei politici.

27. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilități cu privire la securitatea prelucrării datelor cu caracter personal

(prevenire, supraveghere, detectare și prelucrare), precum și operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau al altor împrejurări.

28. Persoana responsabilă de politica de securitate a datelor cu caracter personal va defini clar responsabilitățile și procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională și de funcționare generală, va asigura măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal, va elabora procedurile de clasificare a informației care conține date cu caracter personal astfel încât să fie posibil de întocmit un nomenclator și toate datele cu caracter personal care sunt prelucrate să fie localizate, indiferent de tipul purtătorului de date, va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

29. Protecția datelor cu caracter personal în cadrul FMF (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice și organizatorice de prevenire a prelucrării ilicite a datelor cu caracter personal. Sunt supuse protecției prin mijloace/procedee specifice, toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate pe:

- suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
- sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

VII. SCOPUL MĂSURILOR DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

30. Măsurile de protecție a datelor cu caracter personal sunt dezvoltate pentru:

- a) preîntâmpinarea scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- b) preîntâmpinarea distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
- c) neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- d) eficientizarea resurselor informaționale atât pe suport de hârtie cât și în format electronic.

VIII. PROTECȚIA DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAȚIONALE

31. Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:

- a) preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- c) preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- d) preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor membri ai operatorului/persoanelor împuternicite de către operator,

care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

e) prevenirea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea canalelor VPN;

f) prevenirea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță;

g) prevenirea scurgerii de informații care conțin date cu caracter personal este asigurată prin auditul intern al sistemelor informaționale, **care se efectuează permanent.**

h) stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni cât și pentru cei externi.

IX. PROCEDURILE ORGANIZATORICE ȘI TEHNICE CARE URMEAZĂ A FI RESPECTATE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

32. Măsurile generale de administrare a securității informaționale

a) în cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în **safeuri sau dulapuri metalice care se încuie;**

b) computerele, terminalele de acces și imprimantele sunt deconectate la terminarea sesiunilor de lucru;

c) este asigurată **securitatea punctelor de primire/expediere a corespondenței**, precum și **securitatea contra accesului neautorizat la aparatele fax și de copiere;**

d) este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conțin date cu caracter personal, în scopul împiedicării vizualizării acestora de către persoane neautorizate;

e) mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii;

f) **toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere;**

g) este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

33. Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal

a) accesul în birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare);

b) se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces;

c) perimetrul de securitate a FMF reprezintă perimetru oficiilor în care se prelucrează și sau stochează date cu caracter personal;

- d) perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sunt rezistenți, intrările sunt echipate cu lacăte și semnalizare;
- e) amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesității asigurării securității acestora contra accesului nesanționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri;
- f) ușile și ferestrele se încuie în cazul în care în încăpere lipsesc membrii;
- g) computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine;
- h) accesul în perimetrul de securitate al clădirilor FMF unde se prelucrează și/sau stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținând cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 32 și art. 33 ale Legii privind protecția datelor cu caracter personal nr. 195 din 25 iulie 2024 (în vigoare din 23 august 2026).

34. Identificarea și autentificarea utilizatorilor

- a) este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.
- b) toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conține semnalmentele nivelului de accesibilitate al utilizatorului.
- c) pentru confirmarea ID-ului utilizatorului sunt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice și individuale ale persoanei.
- d) în cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile permise în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă sau se suspendă de administratorul I.T.

35. Identificarea și autentificarea echipamentului

Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal, cu menținerea acestor informații pentru perioada prelucrării.

36. Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:

- identificarea univocă a fiecărui utilizator;
- verificarea autenticității fiecărui utilizator.

37. Utilizarea parolelor în procesul asigurării securității informaționale

Sunt respectate regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor, care includ:

- a) păstrarea confidențialității parolelor, acestea nefiind divulgate niciunei alte persoane, inclusiv personalului IT sau superiorilor ierarhici;
- b) interzicerea înscrierii parolelor pe suport de hârtie sau în fișiere/documente neprotejate, în cazul în care nu se asigură securitatea păstrării acestora;
- c) alegerea unor parole calitative, cu o lungime **minimă de 12 caractere** (sau utilizarea unei fraze-parolă), care nu sunt legate de informația cu caracter personal a utilizatorului (nume,

dată de naștere, IDNP etc.), nu conțin secvențe evidente sau simboluri identice consecutive și nu sunt compuse integral din grupuri de cifre sau litere;

d) **schimbarea parolei se realizează exclusiv atunci când există indicii concrete ale unei posibile compromiteri** a parolei sau a sistemului (acces neautorizat suspectat, incident de securitate confirmat sau suspectat, divulgare accidentală, plecarea din funcție a unui utilizator cu acces partajat etc.), în conformitate cu bunele practici curente de securitate cibernetică (ex. recomandările NIST SP 800-63B), care descurajează rotația periodică forțată fără motiv, aceasta conducând, în practică, la parole mai slabe și mai predictibile;

e) verificarea parolelor noi față de liste cunoscute de parole compromise/uzuale, acolo unde soluția tehnică utilizată permite această funcționalitate;

f) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate) pe echipamentele partajate sau accesibile unor terți.

38. Controlul administrării accesului

Este efectuat controlul sistematic al acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

39. Accesul de la distanță

a) toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sunt documentate, supuse monitorizării și controlului;

b) fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este autorizată de persoanele responsabile și permisă doar utilizatorilor, cărora aceasta le este necesară pentru îndeplinirea obiectivelor stabilite.

40. Limitarea folosirii tehnologiilor fără fir

a) accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului;

b) accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației;

c) folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale FMF.

41. Securitatea electroenergetică

a) echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesancționate, prin montarea lor în nișe speciale;

b) în cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI;

c) sunt implementate sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

42. Controlul instalării și scoaterii componentelor TI

a) este exercitat controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal;

b) informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și **se nimicesc prin metode sigure, evitându-se folosirea funcțiilor standarde de nimicire;**

43. Dezvăluirea datelor cu caracter personal

a) la dezvăluirea formatului electronic al datelor cu caracter personal conținute în sistemele de evidență, prin rețele comunicaționale ori pe alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidență a datelor cu caracter personal este permis doar utilizatorilor autorizați. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice asigurate de destinatar și operator, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți. **În cazul în care rețelele comunicaționale prezintă riscuri pentru confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere** (expediere poștală cu aviz recomandat, înmînarea personală, etc.);

b) **dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale în afara rețelei FMF, la emailuri personale, sunt interzise;**

c) transmiterea datelor cu caracter personal către entități amplasate geografic în stînga Nistrului se realizează exclusiv în scopul organizării și desfășurării activității sportive oficiale (competiții aflate sub egida FMF), cu utilizarea obligatorie a canalelor securizate prevăzute la pct. 36, lit. a) și cu limitarea strictă la datele necesare acestui scop. Sunt interzise orice alte operațiuni de dezvăluire a datelor cu caracter personal către entități din această categorie, în afara celor legate direct de organizarea competițională;

d) procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal;

e) transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. art. 44-50 al Legii privind protecția datelor cu caracter personal nr. 195 din 25 iulie 2024 (în vigoare din 23 august 2026), în special în cazurile cînd tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal;

f) volumul și categoriile datelor cu caracter personal, colectate în scopul ținerii evidenței FMF, este limitat la strictul necesar pentru realizarea scopurilor declarate;

g) accesul la sistemele informaționale gestionate în cadrul FMF, din partea Procuraturii Generale (după caz procuraturile teritoriale/specializate), Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212 Cod de procedură penală. Se explică că în conformitate cu prevederile art. 157 Cod de procedură penală, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice dacă în ele sunt expuse ori adevărate circumstanțe care au importanță pentru cauză, (inclusiv informația stocată în auditul sistemelor informaționale și de evidență), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art. 214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate și răspîndite fără necesitate informație oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată (inclusiv operatorii de date cu caracter personal) au dreptul să se convingă de faptul că aceste date se

colectează pentru procesul penal respectiv, iar în caz contrar să refuze să comunice sau să prezinte date. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate. Urmează a ține cont de faptul că în conformitate cu prevederile art. 8 al Legii privind accesul la informație, datele cu caracter personal fac parte din categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal. În cazul în care avocatul sau persoana împuternicită solicită să ia cunoștință de fișa personală a clientului, aceștia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 și 30 ale Legii privind protecția datelor cu caracter personal nr. 195 din 25 iulie 2024 (în vigoare din 23 august 2026), inclusiv despre răspunderea prevăzută de art. 74 Cod contravențional.

44. Drepturile subiecților de date cu caracter personal

a) în cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile art. 13 și 14 al Legii privind protecția datelor cu caracter personal nr. 195 din 25 iulie 2024 (în vigoare din 23 august 2026), persoanei necesită a-i fi furnizate următoarele informații, exceptând cazul în care el deține deja informațiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul);
- privind scopul concret al prelucrării datelor cu caracter personal colectate;
- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existența drepturilor la informare și de acces la datele colectate;
- de intervenție asupra datelor (în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate;
- dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.

b) subiecților de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoștință de actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neinclunderii sau inclunderii incorecte a unor date, precum și împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în fișele personale (alte materiale), cu excepția cazurilor în care solicitantii își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal;

c) dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entitățile ce asigură menținerea sistemului și/sau prestează servicii externalizate către FMF) tuturor persoanelor supuse prelucrării.

d) în cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaționale principale de stat etc.), modificarea urmând a fi efectuată în toate sistemele informaționale și de evidență gestionate.

45. Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate

- a) accesul în spațiile/perimetrul unde sunt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale /regulamentelor departamentale aprobate;
- b) stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sunt conectate la internet, **nu sunt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă;**
- c) **introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă.** Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul FMF;
- d) stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurată prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

46. Auditul sistemelor informaționale gestionate

- a) se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
 - data și timpul tentativei intrării/ieșirii;
 - ID-ul utilizatorului;
 - rezultatul tentativei de intrare/ieșire - pozitiv sau negativ.
- b) se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
 - data și timpul tentativei de obținere a accesului (executare a operațiunii);
 - denumirea (identificatorul) aplicației sau procesului, ID-ul utilizatorului;
 - specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
 - tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
 - rezultatul tentativei de obținere a accesului (executare a operațiunii) - pozitivă sau negativă.
- c) este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
 - data și timpul modificării competențelor;
 - ID-ul administratorului care a efectuat modificările;
 - ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
- d) se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
 - data și timpul eliberării,
 - denumirea informației și căile de acces la aceasta,
 - specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic), - ID-ul utilizatorului, care a solicitat informația.

47. Asigurarea protecției contra programelor dăunătoare (virusurilor)

Este asigurată protecția contra infiltrării programelor dăunătoare în softurile destinate prelucrării datelor cu caracter personal, prin existența programelor licențiate antivirus.

48. Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal

Se asigură testarea funcționării corecte a funcțiilor de securitate ale sistemelor informaționale de date cu caracter personal (automat la pornirea sistemului și lunar la solicitarea utilizatorului autorizat în acest scop).

49. Gestionarea incidentelor de securitate

- a) personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, **minimum o dată în an**, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate;
- b) angajații FMF informează imediat superiorul ierarhic despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal;
- c) prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității;
- d) până la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris autoritatea națională pentru protecția datelor cu caracter personal despre incidentele de securitate constatate, doar dacă acestea au avut loc.

X. OBLIGAȚIILE ANGAJAȚILOR PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

50. Tuturor salariaților FMF le revin în principal următoarele responsabilități:

- a) verificarea corectitudinii și actualității informației oferite referitor la propriul dosar de angajare și/sau înmatriculare la studii;
- b) informarea responsabililor FMF referitor la orice schimbare a datelor cu caracter personal;
- c) colectarea și prelucrarea cu acuratețe a datelor cu caracter personal, în conformitate cu prevederile legale, de către cei care au acces la acest tip de date.

51. Managerii subdiviziunilor FMF au **obligația de a asigura realizarea anuală a auditului securității în sistemele informaționale de date cu caracter personal.**

XI. DISPOZIȚII FINALE

52. Toată informația care se intenționează a fi dezvăluită și care conține date cu caracter personal urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.

53. Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată

În caz de nerespectare a dispozițiilor Politicii de securitate, Operatorul de date cu caracter personal, persoana împuternicită de către Operator, persoanele responsabile de sistemele de evidență vor purta răspundere juridică, conform prevederilor Codului civil, Codului contravențional și Codului penal.

54. Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe, după caz, semnatarii anexei nr.1, pentru nerespectarea dispozițiilor Politicii de securitate, poartă răspundere, conform legislației în vigoare.

la Politica de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Federația Moldovenească de Fotbal

DECLARAȚIE DE LUARE LA CUNOȘTINȚĂ ȘI ANGAJAMENT DE CONFIDENȚIALITATE

Subsemnatul/subsemnata, _____ (nume, prenume),
 titular al funcției de _____ (funcția/postul),
 în cadrul _____ (subdiviziunea/departamentul FMF),
 IDNP _____, în calitate de persoană cu acces la
 prelucrarea datelor cu caracter personal gestionate de Federația Moldovenească de Fotbal (în
 continuare — **FMF**), prin prezenta:

1. Confirm că am luat cunoștință de conținutul integral al Politicii de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de FMF (în continuare — Politica), aprobată prin Ordinul nr. 683 din 13.07.2026.

2. Declar că am înțeles conținutul Politicii, inclusiv scopurile prelucrării datelor cu caracter personal, categoriile de date prelucrate, precum și măsurile organizatorice și tehnice de securitate stabilite.

3. Mă angajez:

a) să prelucrez datele cu caracter personal la care am acces exclusiv în scopurile determinate, explicite și legitime prevăzute de Politică și de fișa postului/atribuțiile mele funcționale, fără a le utiliza în alte scopuri, personale sau incompatibile cu acestea;

b) să păstrez **confidențialitatea** datelor cu caracter personal la care am acces în exercitarea atribuțiilor de serviciu, atât pe durata raporturilor de muncă/de serviciu cu FMF, cât și **după încetarea acestora**, indiferent de motivul încetării;

c) să nu dezvălui, sub nicio formă, date cu caracter personal către terți neautorizați, inclusiv colegi care nu au atribuții legate de datele respective, cu excepția cazurilor expres prevăzute de Politică sau de legislația în vigoare;

d) să respect regulile privind utilizarea parolelor, identificarea și autentificarea, accesul de la distanță și limitarea folosirii tehnologiilor fără fir;

e) să nu scot din perimetrul de securitate al FMF purtători de date cu caracter personal (documente pe suport de hârtie sau digital) fără o autorizație scrisă prealabilă din partea conducerii;

f) să informez de îndată persoana responsabilă de politica de securitate și/sau superiorul ierarhic despre orice incident de securitate, suspiciune de acces neautorizat, pierdere, divulgare accidentală sau compromitere a datelor cu caracter personal de care iau cunoștință;

g) să respect, în cazul prelucrării datelor cu caracter personal ale minorilor, regimul special de protecție prevăzut în Cap. V din Politică, inclusiv cerințele privind consimțământul reprezentantului legal și limitarea comunicării publice a imaginii minorilor;

h) să mă abțin de la orice acțiune sau inacțiune care ar putea conduce la distrugerea, modificarea, blocarea sau dezvăluirea neautorizată a datelor cu caracter personal.

4. Am fost informat(ă) și înțeleg că **nerespectarea prevederilor Politicii și ale prezentului angajament de confidențialitate atrage răspunderea juridică**, potrivit prevederilor Codului civil, Codului contravențional, Codului penal, precum și ale legislației specifice privind protecția datelor cu caracter personal (Legea nr. 133/2011, respectiv Legea nr. 195/2024, în funcție de perioada aplicabilă), inclusiv posibilitatea sancțiunilor disciplinare aplicabile potrivit raporturilor de muncă/de serviciu cu FMF.

5. Declar că am fost instruit(ă) cu privire la responsabilitățile și obligațiile ce îmi revin în domeniul protecției datelor cu caracter personal și mă angajez să particip la instruirile periodice organizate de FMF în acest sens.

6. Prezentul angajament produce efecte pe toată durata raporturilor mele de muncă/de serviciu/de colaborare cu FMF și **își continuă efectele și după încetarea acestor raporturi**, în ceea ce privește obligația de confidențialitate prevăzută la pct. 3 lit. b).

Data completării

Semnătura

la Politica de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Federația Moldovenească de Fotbal

**REGISTRUL DE EVIDENȚĂ A INSTRUIRII PERSONALULUI
ÎN DOMENIUL PROTECȚIEI DATELOR CU CARACTER PERSONAL**

1. Prezentul registru servește la evidența instruirilor desfășurate în cadrul FMF cu privire la protecția datelor cu caracter personal.
2. Responsabil de organizarea, actualizarea și păstrarea prezentului registru este persoana responsabilă de politica de securitate a datelor cu caracter personal, desemnată conform dispozițiilor din Politică.
3. Registrul se completează la fiecare sesiune de instruire și se păstrează pe toată durata raporturilor de muncă ale persoanei instruite, precum și ulterior, conform termenelor de arhivare prevăzute în Politică.

4. REGISTRUL DE EVIDENȚĂ A INSTRUIRII PERSONALULUI:

Nr.	Nume, prenume	Funcția	Data instruirii	Tip instruire	Rezultat	Semnătura

5. Pentru persoanele care nu participă la instruire, **se va restricționa accesul** la sistemele informaționale de date cu caracter personal, până la parcurgerea corespunzătoare a instruirii, conducerea subdiviziunii respective fiind informată în acest sens.