FEDERAȚIA MOLDOVENEASCĂ DE FOTBAL

POLITICA DE SECURITATE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Chișinău 2017

I. DISPOZIȚII GENERALE

1.1. Prezenta Politică de securitate a datelor cu caracter personal (în continuare "Politica de securitate") prelucrate de către Federația Moldovenească de Fotbal are drept scop stabilirea măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în sistemele informaționale și de a asigura un nivel corespunzător al protecţiei datelor personale a persoanelor vizate.

1.2. Politica de securitate a fost elaborată în conformitate cu prevederile Legii privind protecţia datelor cu caracter personal nr. 133 din 08.06.2011, Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14.12.2010, Convenţiei pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiate la Strasbourg la 28.01.1981, ratificate de Republica Moldova prin Hotărârea Parlamentului nr. 483-XIV din 2.06.1999 şi alte prevederi ale legislației în vigoare a Republicii Moldova.

1.3. Politica de securitate a datelor cu caracter personal se revizuieşte cel puţin o dată în an ca rezultat al modificărilor sau reevaluării componentelor acesteia şi se aprobă de către administratorul federației.

1.4. Noţiunile utilizate în domeniul securităţii datelor cu caracter personal :

date cu caracter personal – orice informaţie 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 identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

categorii speciale de date cu caracter personal – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenenţa socială, datele privind starea de sănătate sau viaţa sexuală, precum şi cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancţiunile contravenţionale;

prelucrarea datelor cu caracter personal – orice operaţiune sau serie de operaţiuni 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, ştergerea sau distrugerea;

sistem de evidenţă 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 funcţionale sau geografice;

operator – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituţie ori organizaţie care, în mod individual sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislaţia în vigoare;

persoană împuternicită de către operator – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor primite de la operator;

terţ – persoană fizică sau persoană juridică de drept public ori de drept privat, alta decât subiectul datelor cu caracter personal, decât operatorul ori persoana împuternicită de către operator şi decât persoana care sub autoritatea directă a operatorului sau a persoanei împuternicite este autorizată să prelucreze date cu caracter personal;

destinatar – orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, căreia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu terţ. Nu sunt considerate destinatari organele din domeniul apărării naţionale, securităţii statului şi ordinii publice, organele de urmărire penală şi instanţele judecătoreşti cărora li se comunică date cu caracter personal în cadrul exercitării competenţelor stabilite de lege;

consimţământul subiectului datelor cu caracter personal – orice manifestare de voinţă liberă, expresă şi necondiţionată, în formă scrisă sau electronică, conform cerinţelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;

II. PRELUCRAREA DATELOR CU CARACTER PERSONAL

2.1. Datele 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 identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale, se împart în două categorii: obişnuite şi speciale.

2.2. Categoria obişnuită a informaţiei prelucrate de către Federația Moldovenească de Fotbal a datelor cu caracter personal, se va efectua în cadrul sistemelor de evidență contabilă, supraveghere video, justiție în domeniul fotbalului; registrelor resurselor umane, de evidență a membrilor și voluntarilor federației, cursurilor de instruire, de licențiere, reclamă și marcheting.

2.3. La desfășurarea de către Federație a unor noi activități cu prelucrarea datele cu caracter personal neincluse în registrele menționate mai sus, vor fi elaborate și aprobate procedurile corespunzătoare, cu notificarea CNPDCP.

2.4. Categoria obişnuită a informaţiei prelucrate se colectează din buletinul de identitate sau un alt act de identitate, carnetul de muncă, documentele de evidenţă militară, diploma de studii, date completate on-line, etc. Deasemenea, categoria obișnuită de date cu caracter personal se regăsește și în datele autobiografice (CV), informaţiile despre salariu, date completate on-line și altele.

2.5. Categoria specială a datelor cu caracter personal o constituie informaţia care dezvăluie originea rasială sau etnică, convingerile politice, religioase, privind starea de sănătate sau viaţa intimă, precum şi cele privind condamnările penale ale unei persoane fizice.

2.6. Prelucrarea de către Federația Moldovenească de Fotbal a categoriei speciale a datelor cu caracter personal se va efectua numai la condițiile art. 6 al Legii nr. 133 din 08.06.2011.

2.7. Prelucrarea datelor cu caracter personal se poate realiza prin mijloace automate, neautomate (manuale) sau mixtă în cadrul unor operaţiuni ori seturi de operaţiuni, fără a fi limitate la acestea, după cum urmează:

a) colectarea - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale şi din orice sursă;

b) înregistrarea - consemnarea datelor cu caracter personal într-un sistem de evidenţă automat ori neautomat, care poate fi registru, fişier automat, bază de date sau orice altă formă de evidenţă organizată, structurată ori ad-hoc sau într-un text, înşiruire de date ori document, indiferent de modalitatea în care se înscriu datele;

c) organizarea - ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuţiilor legale ale operatorului, în scopul eficientizării/ optimizării activităţilor de prelucrare a acestora;

d) stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranţă;

e) adaptarea - transformarea datelor cu caracter personal colectate iniţial, conform criteriilor prestabilite şi scopurilor pentru care au fost colectate;

f) modificarea - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menţinerii caracteristicilor de exactitate, realitate, actualitate;

g) extragerea - scoaterea unei părţi din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat şi distinct de prelucrarea iniţială;

h) consultarea - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operaţiuni sau set de operaţiuni de prelucrare ulterioară;

i) utilizarea - folosirea datelor cu caracter personal, în tot sau în parte, de către şi în interiorul operatorului, împuterniciţilor operatorului ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;

j) dezvăluirea - a face disponibile date cu caracter personal către terţi prin comunicare, transmitere, diseminare sau în orice alt mod;

k) alăturarea - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;

l) combinarea - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate iniţial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;

m) blocarea - întreruperea prelucrării datelor cu caracter personal;

n) ştergerea - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidenţe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistenţa, inexactitatea;

o) transformarea - operaţiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;

p) distrugerea - aducerea la stare de neântrebuinţare, în condiţiile legii, definitivă şi irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

2.8. Prelucrarea datelor cu caracter personal se face cu respectarea următoarelor principii:

a) Legalitatea: Prelucrarea datelor cu caracter personal se face în temeiul și în conformitate cu prevederile legale.

b) Scopul bine-determinat: Orice prelucrare de date cu caracter personal se face în scopuri bine determinate, explicite și legitime, adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate.

c) Confidenţialitatea: Federația la prelucrarea datelor cu caracter personal, la semnarea contractului, va semna și clauza de confidenţialitate.

d) Consimţământul persoanei vizate: Orice prelucrare de date cu caracter personal a clienţilor/angajaților poate fi efectuată numai dacă persoana vizată şi-a dat consimţământul pentru acea prelucrare.

e) Protejarea persoanelor vizate: Persoanele vizate au dreptul de acces la datele care sunt prelucrate, de a interveni asupra acestora, de opoziţie și de a nu fi supus unei decizii individuale, precum și dreptul de a se adresa Centrului Naţional pentru Protecţia Datelor cu Caracter Personal sau instanţei de judecată pentru apărarea oricăror drepturi garantate de lege, care le-au fost încălcate.

f) Securitatea: Măsurile de securitate a datelor cu caracter personal sunt stabilite astfel încât să asigure un nivel adecvat de securitate a datelor cu caracter personal procesate.

2.9. La depunerea cererii privind angajarea și ulterior semnarea unui contract individual de muncă, precum și alte tipuri de contracte, ori documente, după caz, precum și perfectarea documentelor pentru obținerea unui card bancar salarial, subiectul datelor cu caracter personal i se solicită consâmțământul în scris privind prelucrarea datelor cu caracter personal întru realizarea contractului individual de muncă precum și alte tipuri de contracte, ori documente, după caz.

2.10. Înainte de a semna acordul privind prelucrarea datelor personale, subiectului datelor cu caracter personal vor fi aduse la cunoștință prevederile art. 12 - 16 ale Legii nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal. Și numai după luarea cunoștinței vor fi înregistarte datele personale ale subuiectului în registrele corespunzătoare, cu prelucrarea lor posterioară.

2.11. Refuzul candidatului/solicitantului menționat la pct. 2.9 de a semna în scris un acord privind prelucrarea datelor cu caracter personal se echivalează cu imposibilitatea angajării în câmpul muncii sau derulării unui alt contract, cu exepția situațiilor menționate în alin. (5) al art. 5 al Legii Nr. 133 din 08 iulie 2011, când acordul în scris nu este obligatoriu pentru:

a) executarea unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înaintea încheierii contractului, la cererea acestuia, cu exepția când se preluncrează și IDNPul subiectul datelor cu caracter personal ;

b) îndeplinirea unei obligaţii care îi revine operatorului conform legii;

c) protejarea vieţii, integrităţii fizice sau a sănătăţii subiectului datelor cu caracter personal;

d) executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terţul căruia îi sunt dezvăluite datele cu caracter personal;

e) realizarea unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele cu caracter personal, cu condiţia ca acest interes să nu prejudicieze interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal;

f) scopuri statistice, de cercetare istorică sau ştiinţifică, cu condiţia ca datele cu caracter personal să rămână anonime pe toată durata prelucrării.

2.12. În conformitate cu prevederile alin. (2) al art. 5 al Legii nr. 133 din 08.07.2011 consimţământul privind prelucrarea datelor cu caracter personal poate fi retras în orice

moment de către subiectul datelor cu caracter personal. Totodată, retragerea consimţământului nu poate avea efect retroactiv.

2.13. Angajaților federației ***se interzice*** de a colecta, stoca, etc. și transmite terțelor părți date cu caracter personal aflate în cadrul executării funcției, dacă funcția deținută nu prevede așa drepturi sau legislația nu prevede expres transmiterea unor așa date terțelor părți, fără consințământul subiectului datelor cu caracter personal ale cărui date vor fi transmise (dezvăluite).

2.14. Federația Moldovenească de Fotbal colectează deasemenea date personale prin intermediul fmf.md prin trei modalitati:

- direct de la utilizator: în momentul abonării la serviciile Fan club cu prelucrarea informațiilor cu caracter personal (adresa de mail, nume, prenume, etc.);
- din raportul de trafic al serverului: în momentul vizitării fmf.md, se furnizează anumite informații despre utilizator, cum ar fi IP, ora vizitei, locul de unde s-a intrat, durata vizitei;
- prin intermediul cookie-urilor: când utilizatorul vizitează fmf.md este posibil să fie trimis un cookie pentru a facilita stocarea și urmărirea peferințelor utilizatorului.

III. DREPTUL SUBIECTULUI DATELOR CU CARACTER PERSONAL

3.1. Dreptul de acces la datele cu caracter personal

Orice subiect al datelor cu caracter personal are dreptul să obţină de la operator, la cerere, fără întârziere şi în mod gratuit:

a) confirmarea faptului că datele care îl privesc sunt sau nu sunt prelucrate de acesta, de asemenea informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;

b) comunicarea, într-o formă inteligibilă şi într-un mod care nu necesită un echipament suplimentar, a datelor cu caracter personal care fac obiectul prelucrării, precum şi a oricărei informaţii disponibile privind originea acestor date;

c) informaţii privind principiile de funcţionare a mecanismului prin care se efectuează prelucrarea automatizată a datelor care vizează subiectul datelor cu caracter personal;

d) informaţii cu privire la consecinţele juridice generate de prelucrarea datelor cu caracter personal pentru subiectul acestor date;

e) informaţii privind modul de exercitare a dreptului de intervenţie asupra datelor cu caracter personal.

3.2. Dreptul de intervenţie asupra datelor cu caracter personal

Orice subiect al datelor cu caracter personal are dreptul de a obţine de la operator sau persoana împuternicită de către acesta, la cerere şi în mod gratuit:

a) rectificarea, actualizarea, blocarea sau ştergerea datelor cu caracter personal a căror prelucrare contravine Legii nr. 133 din 08.07.2011, înspecial datorită caracterului incomplet sau inexact al datelor;

b) notificarea terţilor cărora le-au fost dezvăluite datele cu caracter personal despre operaţiunile efectuate conform lit. a), exceptând cazurile când această notificare se

dovedeşte a fi imposibilă sau presupune un efort disproporţionat faţă de interesul legitim care ar putea fi lezat.

3.3. Dreptul de opoziţie al subiectului datelor cu caracter personal

(1) Subiectul datelor cu caracter personal are dreptul de a se opune în orice moment, în mod gratuit, din motive întemeiate şi legitime legate de situaţia sa particulară, ca datele cu caracter personal care îl vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care legea stabileşte altfel. Dacă opoziţia este justificată, prelucrarea efectuată de operator nu mai poate viza aceste date.

(2) Subiectul datelor cu caracter personal are dreptul de a se opune în orice moment, în mod gratuit şi fără nici o justificare, ca datele care îl vizează să fie prelucrate pentru prospectare comercială. Operatorul sau persoana împuternicită de către operator este obligată să informeze subiectul despre dreptul de a se opune unei astfel de lucrări înaintea dezvăluirii către terţi a datelor sale cu caracter personal.

(3) Dreptul de opoziţie al subiectului datelor cu caracter personal, care le poate exercita printr-o cerere scrisă adresată către: ***Federația Moldovenească de Fotbal, str. str. Tricolorului 39, or. CHIȘINĂU, MD-2012, Republica Moldova .***

3.4. Accesul la justiţie

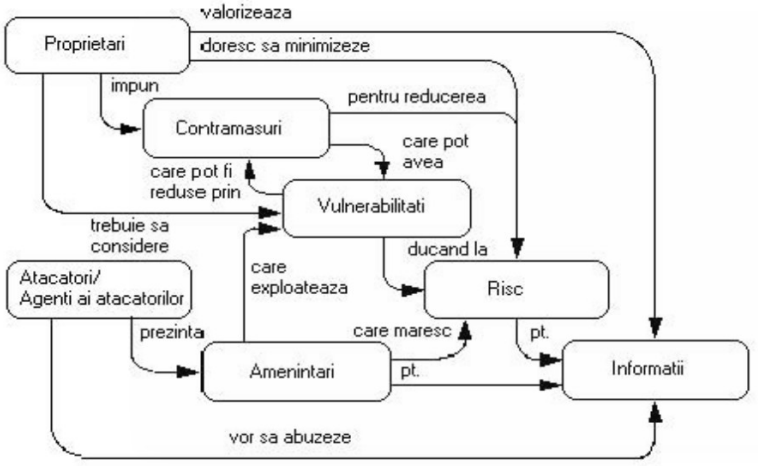
Orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal efectuată ilegal sau căreia i-au fost încălcate drepturile şi interesele garantate de prezenta lege are dreptul de a sesiza instanţa de judecată pentru repararea prejudiciilor materiale şi morale.

IV. PERICOLELE, RISCURILE ŞI VULNERABILITATEA SISTEMELOR INFORMAȚIONALE DE EVIDENȚĂ A DATELOR CU CARACTER PERSONAL PRELUCRATE

4.1. Securitatea informaţiei se defineşte ca capacitatea sistemului de relucrare a informaţiei de a asigura în anumită perioadă de timp a posibilităţii de executare a cerinţelor stabilite după mărimea probabilităţii realizării evenimentelor, manifestate în:

- exodul informaţiei;
- modificarea sau pierderea de date, ce prezintă anumită valoare pentru deţinător.

4.2. Reprezentarea schematică a conceptelor privind securitatea sistemelor de informații compiuterizate și relațiile dintre acestea sunt prezentate în figura de mai jos.



4.3. Prin **pericol** se înţelege un eveniment sau o acţiune posibilă, orientată spre cauzarea prejudiciului resurselor sau infrastructurii informaţionale. Pericole principale pentru securitatea informaţională sunt:

a) colectarea şi utilizarea ilegală a informaţiei;

b) încălcarea tehnologiei de prelucrare a informaţiei;

c) implementarea în produsele software şi hardware a componentelor, care realizează funcţii, neprevăzute în documentaţia la aceste produse;

d) elaborarea şi răspândirea programelor, care afectează funcţionarea normală a sistemelor informaţionale şi informaţionale de telecomunicaţii, precum şi a sistemelor securităţii informaţionale;

e) compromiterea cheilor şi mijloacelor de protecţie criptografică a informaţiei;

f) influenţarea asupra sistemelor cu parolă-cheie de protecţie a sistemelor automatizate de prelucrare şi transmitere a informaţiei;

g) implementarea dispozitivelor electronice pentru interceptarea informaţiei în mijloacele tehnice de prelucrare, păstrare şi transmitere a informaţiei prin canalele de comunicaţii;

h) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informaţie mecanice sau a altor suporturi;

i) utilizarea tehnologiilor informaţionale autohtone şi străine necertificate;

4.4. Surse ale pericolelor:

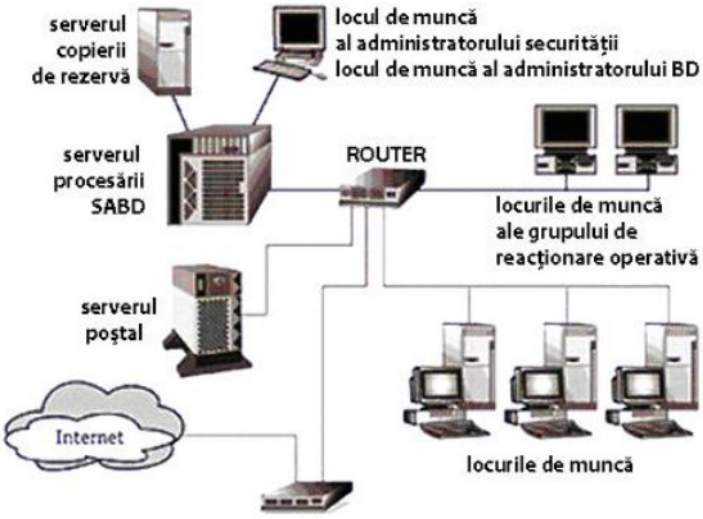
a) infractorii;

b) precum şi utilizatorii de rea-credinţă.

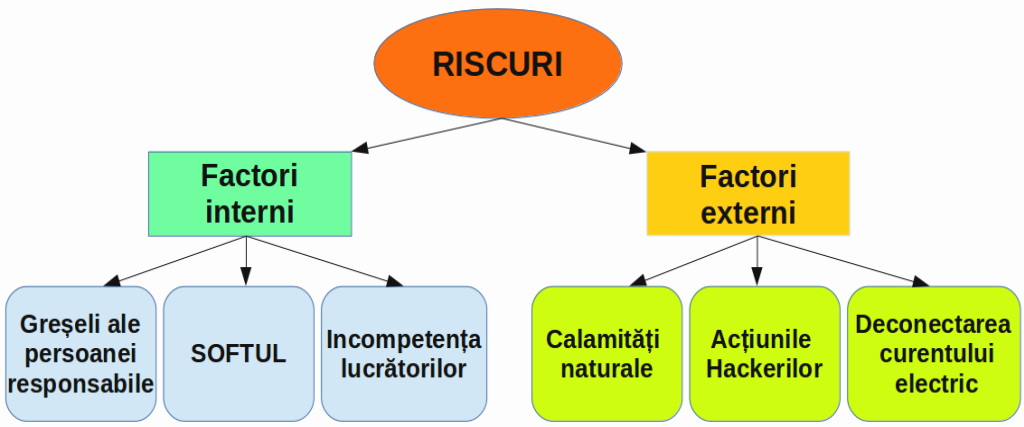
4.5. Personalul care administrează sistemul sau doar folosește calculatorul reprezintă cea mai mare vulnerabilitate pentru securitatea acestuia, deoadece dacă se va decide să profite, în mod fraudulos, de oportunităţile sale, pentru obţinerea unor beneficii nemeritate, amplifică probabilitatea unor breşe de securitate în sistem, care se va afla în pericol.

4.6. Deasemenea şi programatorii sau persoanele care întreţin sau repară calculatorul, pot fi corupţi sau forţaţi să divulge parole, informaţii sau căi de acces, cu alte cuvinte să compromită securitatea computerului.

4.7. Obiecte ale pericolelor - sunt resursele informaţionale sau infrastructura informaţională.



4.8. Riscul este evenimentul capabil sa exercite o influenta asupra sistemului informațional gestionat



4.9. Vulnerabilitatea sistemului:

– posibilitatea modificării sau distrugerii informației, adică atacul la integritatea ei fizică;

– posibilitatea folosirii neautorizate a informațiilor, adică scurgerea lor.

4.10. Toate calculatoarele emit radiaţii electrice şi electromagnetice care pot fi interceptate, analizate şi descifrate. De aceea, informaţiile stocate şi transmise în și din sistemele de calcul şi reţele devin vulnerabile.

4.11. Internetul este o structură deschisă la care se poate conecta un număr mare de calculatoare, fiind deci greu de controlat.

4.12. Calculatoarele sunt foarte vulnerabile la dezastrele naturale şi la ameninţările provenite din mediul înconjurător.

4.13. Pericolele majore ca incendiile, inundaţiile, cutremurele, fulgerele şi căderile de tensiune pot distruge echipamente de calcul şi datele utilizatorilor. Praful, umezeala şi temperatura variabilă pot avea, de asemenea, fecte distructive. Unele tipuri de defecţiuni hardware ce potcompromite securitatea unui întreg sistem de calcul.

4.14. Liniile de comunicaţie şi conexiunile reţelelor sunt foarte vulnerabile la atacuri. Adesea este mai uşor să pătrunzi într-un sistem prin intermediul reţelei, decât din interior. Hackerii sunt pasionați ai informaticii, care, de obicei au ca scop „spargerea anumitor coduri, bazede date, etc., fiind considerați infractori, în majoritatea statelor lumii.

V. MĂSURI DE SECURITATE ŞI MIJLOACELOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

5.1. În cadrul activităţii profesionale, Federația Moldovenească de Fotbal, gestionează și utilizează registrele menționate în pct. 2.2 al prezentei Politici de securitate, exclusiv în scopurile pentru care ele sunt create.

5.2. Accesul la datele personale prelucrate în registrele de evidență va fi restricționat, în dependență de funcția deținută, obligațiuni și împuterniciri, având la bază principiul: acces numai la informația necesară pentru executarea funcției, conform organigramei federației, cu semnarea unui acord de confidențialitate separat sau prin introducerea clauzei de confidențialitate, în contractul individual de muncă.

5.3. În domeniul securității datelor cu caracter personal, prin ordine pe Federație:

a) vor fi numiți persoanele responsabile de implementarea și monitorizarea respectării prevederilor Politicii de securitate pe Federație pentru fiecare registru notificat;

b) privind aprobarea listei funcțiilor federației admise la prelucrarea datelor cu caracter personal și a limitelor/restricțiilor impuse;

c) privind numirea comisiei de audit privind respectarea prevederilor Politicii de securitate și a legistației privind securitatea datelor cu caracter personal.

5.4. Persoanele responsabile de realizarea politicii de securitate a datelor cu caracter personal pentru registrele notificate vor fi asigurate și vor dispune de resurse suficiente (timp, resurse umane, echipament și buget) și vor avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în cadrul registrului notificat, în conformitate cu legislația în vigoare.

5.5. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii și administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole.

5.6. Este autorizat accesul la sistemele informaţionale de date cu caracter personal în conformitate cu politica de administrare a accesului stabilită de deţinătorul de date cu caracter personal, în conformitate cu restricțiile din ordinul pe Federație privind accesul angajaților la date personale.

5.7. Drepturile de acces ale utilizatorilor la sistemul informaţional de date cu caracter personal sunt revizuite cu regularitate pentru asigurarea faptului, că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni) și după oricare schimbare de statut al utilizatorului.

5.8. Se autorizează de către deţinătorii de date cu caracter personal realizarea fluxurilor informaţionale în procesul transmiterii acestora în interiorul și în afara sistemului informaţional de date cu caracter personal.

5.9. Accesul fără fir la sistemul informaţional de date cu caracter personal este documentat, supus monitorizării și controlului și este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.

Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale registrului corespunzător de date cu caracter personal și numai după asigurarea condițiilor de securitate.

5.10. Cerințele concrete față de prelucrarea datelor cu caracter personal și față de mijloacele de prelucrare vor fi stabilite în regulamentele de realizare a Politicii de securitate pentru fiecare registru în parte.

5.11. Regulamentele privind realizarea politicii de securitate a prelucrării datelor cu caracter personal se anexează și sunt parte integrală a prezentei Politici de securitate.

VI. TRANSMITEREA DATELOR CU CARACTER PERSONAL

6.1. Federațiea este obligată să comunice informaţiile solicitate, în termen de 15 zile de la data primirii cererii, cu respectarea opţiunii solicitantului, ca răspunsul să fie transmis la o anumită adresă, care poate fi şi de poştă electronică sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai solicitantului.

6.2. În cazul în care o persoană nu a primit răspuns din partea operatorului la cererea formulată în termen de 15 zile sau este nemulţumită de conţinutul răspunsului primit, se poate adresa cu o plângere către CNPDCP.

6.3. Transmiterea datelor cu caracter personal terțelor părți, care conform prevederilor legale nu sunt obligatorii (alți operatori de date cu caracter personal) se efectuează numai după semnarea acordul în scris al subiectului de date cu caracter personal ale cărui date personale urmează a fi transmise. În acord se menționează clar în baza la ce document și cui îi va fi dezvăluită informația, întru a exclude cazul de transmitere și altor operatori sau persoane neautorizate în baza acordului semnat.

Acordul nu se solicită, dacă pentru realizarea contractul încheiat cu subiectul de date cu caracter personal, necesită și prevede transmiterea datelor cu caracter personal terțelor părți, cu excepția cazului când se prelucrează și IDNPul.

6.4. Transmiterea datelor cu caracter personal organelor de stat, care conform prevederilor legale sunt obligatorii (FISC, CNAS, CNAM și altele, în dependență de cerințele legislației genurilor de activitate desfășurate de Federație) se efectuează fără a solicita acordul subiectului de date cu caracter personal.

6.5. Mesajele electronice şi documentele nu sunt private cât timp sunt create şi/sau stocate pe calculatorul de serviciu. O copie de siguranţă a tuturor emailurilor transmise sau primite pe adresele profesionale, se va păstra și pe calculatorul, dacă este cazul, iar după expirarea necesității, mailurile de pe serverul poștei vor fi sterse.

6.6. Internetul oferă multe opţiuni de comunicare electronică gratuită. Se consideră că acest sistem de comunicare electronică nu corespund cerinţelor de protecţie a datelor cu caracter personal. Deaceia, pentru a transmite datele personale prin mail, persoana care intenționează să transmită datele personale, va solicita acordul prealabil al clientului/angajatului Federației trimitând inițial un mail cu așa solicitare. Și numai după confirmare va transmite datele.

6.7. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmânarea personală, etc.).

VII. AUDITUL ȘI DĂRILE DE SEAMĂ

7.1. În perioada 1-15 decembrie, anual, comisia numită prin ordinul președintelui federației verifică cel puţin îndeplinirea măsurilor tehnice şi/sau organizaţionale luate pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea în procesul prelucrării datelor cu caracter personal a sistemelor de telecomunicaţii şi/sau efectuarea îmbunătăţirilor, în caz de necesitate.

7.2. Rezultatele auditului securității în sistemul informaţional de date cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidenţialităţii și integrităţii acesto

7.3. Durata stocării rezultatelor auditului securităţii în sistemul informaţional de date cu caracter personal nu este mai mică de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

7.4. Prelucrarea incidentelor va include nu doar depistarea, dar şi analiza, preântâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

7.5. Anual, către 31 ianuarie, responsabilul de Politica de securitate prezintă Centrului Naţional pentru Protecţia Datelor cu Caracter Personal raportul generalizat despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal.

VIII. DISPOZIŢII FINALE

8.1. Prezenta Politică de securitate și Regulamentele anexate se revizuesc periodic, cel puțin o dată în an, în caz de incidente de securitate, precum și la necesitate.

8.2. Politică de securitate și Regulamentele anexate se adus la cunoştinţa angajaților contra semnăturii.

Anexe: **1.** Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în registrului resurselor umane.

2. Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în sistemului de evidență contabilă

3. Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în sistemul de supraveghere video.

4. Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în cadrul registrului membrilor federației.

5. Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în cadrul registrului voluntarilor.

6. Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în cadrul registrului licențelor eliberate de FMF.

7. Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în cadrul Cursurilor de instruire.

8. Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în cadrul registrului reclamă și marcheting.

9. Regulamentul privind realizarea politicii de securitate a prelucrării datelor cu caracter personal în cadrul organelor judiciare ale FMF.

Președinte **Pavel CEBANU**