Aprobat
prin Hotărîrea Guvernului Nr.____
din "___"_____20__

REGULAMENTUL
cu privire Sistemul informaţional automatizat
"Registrul persoanelor reţinute, arestate şi condamnate"

I. Dispoziţii generale

1. Regulamentul cu privire la Sistemul informaţional automatizat „Registrul persoanelor reţinute, arestate şi condamnate" (în continuare – Regulament) stabileşte modul de organizare şi funcţionare a resurselor informaţionale a Departamentului instituţiilor penitenciare ca parte integrantă a Sistemului informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni, modul de asigurare informaţională a organelor de drept în combaterea criminalităţii prin utilizarea informaţiei operative şi veridice referitor la persoanele aflate în detenţie în instituţiile penitenciare, cerinţele faţă de protecţia datelor de categorie specială cu caracter personal la colectarea, acumularea, actualizarea, păstrarea, prelucrarea şi transmiterea informaţiilor privitor la persoanele deţinute.

2. Noţiunile utilizate în prezentul Regulament au semnificaţia prevăzută în art.2 din Legea nr. 216-XV din 29 mai 2003 cu privire la Sistemul informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni, art.3 din Legea nr.71 din 22 martie 2007 cu privire la registre, art.3 din Legea nr.133 din 08 iulie 2011 privind protecţia datelor cu caracter personal şi în Concepţia Sistemului informaţional automatizat "Registrul persoanelor reţinute, arestate şi condamnate", aprobată prin Hotărîrea Guvernului nr. 25 din 18 ianuarie 2008.

În sensul prezentului Regulament se definesc următoarele noţiuni:

administrator al SIA RPRAC – subdiviziunea responsabilă de gestionarea şi operarea resurselor informaţionale ale Registrului;

complex de mijloace software şi hardware – totalitatea programelor şi mijloacelor tehnice care asigură realizarea proceselor informaţionale;

utilizator – persoana fizică sau juridică ale cărei atribuţii de serviciu presupun acţiuni de prezentare, primire, păstrare, precum şi utilizare a informaţiei cu caracter criminal,

3. Sistemul informaţional automatizat registrul persoanelor reţinute, arestate şi condamnate (în continuare – SIA RPRAC), include totalitatea informaţiei de categorie specială de date cu caracter personal a persoanelor deţinute în instituţiile penitenciare.

4. SIA RPRAC creează un spaţiu informaional unitar şi constituie unica sursă oficială de informaţii cu referire la persoanele aflate în detenţie în instituţiile sistemului penitenciar pentru participanţii la SIA RPRAC şi pentru alte sisteme informaţionale ale autorităţilor administraţiei publice centrale care utilizează şi prelucrează astfel de date. Datele SIA RPRAC se consideră corecte şi veridice pînă la proba contrarie.

II. Subiecţii raporturilor juridice în domeniul creării şi funcţionării SIA RPRAC

5. SIA RPRAC este un sistem informaţional automatizat specializat şi este parte integrantă a Sistemul informaţional integrat al organelor de drept (SIIOD). Proprietarul SIA RPRAC este statul.

6. Departamentul Instituţiilor Penitenciare al Ministerului Justiţiei este deţinătorul şi posesorul SIA RPRAC şi asigură condiţiile juridice, organizatorice şi financiare pentru crearea şi gestionarea acestuia.

7. Registratorii şi subregistratorii SIA RPRAC sînt serviciile autorizate din cadrul structurii organizatorice ale instituţiilor sistemului penitenciar, care, în procesul de îndeplinire a funcţiilor lor, asigură formarea resurselor informaţionale caracteristice pentru domeniul de activitate.

8. Administratorul SIA RPRAC este serviciul autorizat al Departamentului Instituțiilor Penitenciare responsabil de gestionarea şi operarea resurselor informaţionale ale SIA RPRAC.

III. Gestionarea și asigurarea funcționării SIA RPRAC

9. SIA RPRAC se gestionează în format electronic şi se realizează prin intermediul constituirii resurselor informaţionale, care reprezintă totalitatea informaţiei sistematizate cu privire la persoanele aflate în detenţie în sistemul penitenciar.

10. SIA RPRAC se gestionează în limba de stat.

11. Introducerea informaţiei în SIA RPRAC se efectuează în conformitate cu datele din dosarul personal al deţinutului şi registrelor de evidenţă a penitenciarului. Evidenţa obiectelor informaţionale se gestionează conform ghidului de utilizare al SIA RPRAC.

12. Datele se păstrează în SIA RPRAC în ordine cronologică, ceea ce asigură posibilitatea obţinerii datelor cu privire la persoanele aflate în detenţie în perioadele determinate.

13. Pentru asigurarea funcţionării eficiente şi neîntrerupte a SIA RPRAC, schimbul informaţional de date între participanţii la SIA RPRAC este asigurat în regim nonstop.

14. Schimbul informaţional se efectuează numai cu utilizarea complexului de mijloace software şi hardware specializat.

15. Radierea datelor de categorie specială cu caracter personal din SIA RPRAC se efectuează de către administratorul SIA RPRAC la solicitarea registratorului.

16. Modul de colectare, prelucrare, păstrare şi utilizare a datelor de categorie specială cu caracter personal din SIA RPRAC se va efectua în conformitate cu prevederile Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal şi Regulamentul cu privire la implementarea măsurilor de securitate şi ghidul de utilizare ale SIA RPRAC, elaborate de posesor.

17. Păstrarea SIA RPRAC este asigurată de posesor pînă la adoptarea deciziei de lichidare a sistemului.

18. Datele din SIA RPRAC rămîn la păstrare cu statut de document de arhivă de la data încetării utilizării acestora în scopul apărării naţionale, securităţii statului, menţinerii ordinii publice, protecţiei drepturilor şi libertăţilor omului.

IV. Obligaţiile şi drepturile participanţilor la SIA RPRAC

19. În funcţie de rol, registratorii, subregistratorii şi alţi participanţi la SIA RPRAC sînt obligaţi:

1) să asigure înregistrarea, colectarea, acumularea, prelucrarea şi transmiterea informaţiilor despre persoanele deţinute, în banca centrală de date a SIA RPRAC, conform formatelor stabilite de legislaţie, precum şi în termenii indicaţi în ghidul de utilizare a SIA RPRAC;

2) să verifice respectarea condiţiilor de înregistrare, evidenţă şi utilizare a informaţiei cu caracter personal şi cu referire la detenţie;

3) să asigure corectitudinea, veridicitatea şi autenticitatea datelor colectate şi transmise pentru a fi introduse în SIA RPRAC şi actualizarea acestora;

4) la solicitarea administratorului SIA RPRAC, să prezinte în termen de 2 zile lucrătoare, informaţiile suplimentare necesare pentru completarea datelor din banca centrală de date a SIA RPRAC;

5) să asigure şi să efectueze controlul sistemului de securitate, să fixeze cazurile şi tentativele de încălcare a acestuia, precum şi să întreprindă măsurile ce se impun pentru prevenirea şi lichidarea consecinţelor;

6) să asigure securitatea accesului la informația stocată în banca centrală de date a SIA RPRAC, respectarea condițiilor de securitate şi regulilor de exploatare a SIA RPRAC;

7) să asigure, să organizeze şi să amenajeze locuri de muncă corespunzătoare pentru persoanele autorizate, responsabile de acumularea, prezentarea şi recepţionarea informaţiei cu privire la detenţie;

8) să asigure condiţiile necesare pentru păstrarea în siguranţă a suporturilor materiale şi a copiilor de rezervă, precum şi pentru excluderea accesului persoanelor neutorizate la suporturile respective;

9) să implementeze protecţia antivirus şi antispam;

10) să efectueze deservirea tehnică a componentelor, să înlăture defecţiunile tehnice a locurilor de muncă automatizate conectate la SIA RPRAC;

11) să utilizeze informaţia obţinută din banca centrală de date a SIA RPRAC doar în scopurile stabilite de legislaţia în vigoare;

12) să înştiinţeze imediat, în formă scrisă, verbală sau prin orice alte mijloace de comunicare, administratorul SIA RPRAC despre cazurile de încălcare a securităţii informaţionale a SIA RPRAC;

13) imediat să aducă la cunoştinţa administratorului SIA RPRAC orice situaţie de forţă majoră apărută, care ar putea influenţa în mod negativ exercitarea funcţiilor participantului.

20. Fiecare registrator, subregistrator sau alt participant au următoarele drepturi:

1) să participe la crearea, implementarea şi dezvoltarea SIA RPRAC;

2) să înainteze propuneri cu privire la modificarea cadrului normativ existent care reglementează funcţionarea SIA RPRAC;

3) să solicite şi să primească gratuit informaţia cu privire la ispăşirea pedepsei în cadrul instituţiilor penitenciare, conţinută în banca centrală de date a SIA RPRAC, precum şi rapoartele statistice generalizate;

4) să solicite şi să primească de la administratorul SIA RPRAC ajutor metodologic şi practic pe problemele ce ţin de funcţionarea SIA RPRAC;

5) să prezinte propuneri în modul stabilit de legislaţie administratorului SIA RPRAC privind perfecţionarea şi eficientizarea funcţionării SIA RPRAC.

V. Obligaţiile şi drepturile administratorului la SIA RPRAC

21. Administratorul SIA RPRAC este obligat:

1) să asigure funcţionarea şi gestionarea SIA RPRAC în conformitate cu actele normative în vigoare;

2) să asigure suportul metodologic şi practic pentru toţi registratorii la SIA RPRAC pe problemele legate de ţinerea, actualizarea şi utilizarea SIA RPRAC;

3) să asigure colectarea informaţiilor de la participanţi, stocarea lor în banca centrală de date, menţinerea şi actualizarea SIA RPRAC în baza informaţiei colectate;

4) să acorde utilizatorului SIA RPRAC acces la informaţia din banca centrală de date a SIA RPRAC în conformitate cu legislaţia în vigoare şi nivelului de acces. În caz de modificare a drepturilor de acces, administratorul va lua decizia cu privire la reconfigurarea acestora în caz de necesitate;

5) să asigure utilizatorului autorizat, accesul la datele incluse în SIA RPRAC;

6) să asigure asistenţă informaţională a utilizatorilor SIA RPRAC în modul stabilit;

7) să efectueze măsurile necesare privind protecţia şi confidenţialitatea informaţiilor din SIA RPRAC, inclusiv împotriva accesului, corectării, modificării şi transmiterii neautorizate;

8) să asigure măsurile tehnico - organizatorice necesare pentru protecţia datelor în conformitate cu cerinţele privind protecţia datelor stocate în SIA RPRAC şi respectarea acestor măsuri;

9) să protejeze datele colectate, echipamentele tehnice şi produsele de program utilizate pentru administrarea acestora, asigurînd securitatea şi integritatea datelor conţinute în banca centrală de date a SIA RPRAC împotriva riscurilor de pierdere, distrugere, precum şi împotriva folosirii neautorizate sau divulgării lor;

10) să efectueze monitorizarea şi supravegherea accesărilor informaţiei din SIA RPRAC;

11) să efectueze auditul securităţii SIA RPRAC, care conţine categorii speciale de date cu caracter personal;

12) să execute, o dată la 30 de zile calendaristice, copiile de siguranţă ale informaţiilor care conţin datele din Sistem şi softurilor folosite pentru prelucrările automatizate ale datelor din SIA RPRAC pe suport material, care se păstrează în locuri protejate, şi să asigure restaurarea informaţiilor în caz de necesitate;

13) să instaleze mijloacele software la locurile de muncă autorizate ale registratorilor şi să acorde suportul necesar pentru conectarea acestora la banca centrală de date a SIA RPRAC;

14) să acorde asistenţă persoanelor autorizate care au acces la SIA RPRAC referitor la utilizarea complexului de mijloace software şi hardware;

15) să informeze registratorii despre modificările condiţiilor tehnice de funcţionare a SIA RPRAC.

22. Administratorul Sistemului este în dreptl:

1) să supravegheze respectarea cerinţelor de securitate informaţională de către registratori, să fixeze cazurile şi tentativele de încălcare a acestora, precum şi să întreprindă măsurile necesare pentru prevenirea şi lichidarea consecinţelor;

2) să solicite de la registratori informaţiile necesare pentru completarea datelor din banca centrală de date a SIA RPRAC;

3) să iniţieze procedura de suspendare a drepturilor de acces la datele incluse în SIA RPRAC în cazurile de nerespectare a regulilor, standardelor şi normelor general acceptate în domeniul securităţii informaţionale;

4) să stabilească cerinţe faţă de mijloacele tehnice, canalele telecomunicaţionale şi software la locurile automatizate de muncă ale participanţilor;

5) să perfecţioneze şi să asigure eficientizarea funcţionării SIA RPRAC.

VI. Regimul juridic de utilizare a datelor din SIA RPRAC

23. Accesul la baza de date a SIA RPRAC este condiţionat de exercitarea corespunzătoare a atribuţiilor de serviciu de către utilizator. Astfel, registratorul sau subregistratorul are acces tehnic la datele din SIA RPRAC, ceea ce presupune introducerea, modificarea şi radierea informaţiei înregistrate de ei. Restul utilizatorilor au acces informaţional la datele din SIA RPRAC, ceea ce presupune vizualizarea informaţiei numai în formatul individual permis pentru fiecare utilizator în parte. În unele cazuri registratorul sau subregistratorul poate avea rol de utilizator cu acces informaţional la informaţia la care accesul pentru ei este limitat.

24. Acordarea accesului la datele din SIA RPRAC se efectuează de către administratorul SIA RPRAC în baza acordurilor încheiate între posesorul SIA RPRAC şi destinatarul datelor din SIA RPRAC.

25. Extrasele din SIA RPRAC, adeverinţele şi documentele se eliberează doar de către posesorul SIA RPRAC şi poartă semnătura acestuia. Documentele electronice poartă semnătura digitală a posesorului SIA RPRAC, în modul stabilit de legislaţie.

26. Se interzice utilizarea datelor din SIA RPRAC în alte scopuri decît cele prevăzute de legislaţie.

27. Participanţii SIA RPRAC nu sînt în drept să modifice datele obţinute din SIA RPRAC, iar la utilizarea acestora este obligat să indice sursa lor.

VII. Modalitatea de conectare/deconectare a participanţilor la SIA RPRAC

28. Accesul la informaţia din SIA RPRAC pentru participanţi, se acordă de către administratorul SIA RPRAC, în temeiul demersului oficial cu specificarea numărului necesar de locuri automatizate de muncă, a setului de date speciale cu caracter personal şi a datelor personale ale utilizatorilor.

29. Administratorul SIA RPRAC execută lucrările necesare de instalare a mijloacelor software la locurile de muncă autorizate ale registratorilor şi acordă suport la conectarea acestora la banca centrală de date a SIA RPRAC, cu semnarea între părţi a actului de instalare-primire a locurilor de muncă.

30. Funcţionarea SIA RPRAC este suspendată de către administratorul SIA RPRAC în următoarele cazuri:

1) în timpul efectuării lucrărilor de profilaxie ale complexului de mijloace software şi hardware ale SIA RPRAC;

2) la apariţia circumstanţelor de forţă majoră;

3) la încălcarea măsurilor de securitate informaţională, dacă aceasta prezintă pericol pentru funcţionarea SIA RPRAC.

31. Lucrările de prifilaxie în complexul de mijloace software şi hardware ale băncii centrale de date a SIA RPRAC se efectuează după înştiinţarea în scris a participanţilor cu 2 zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora.

32. În cazul apariţiei circumstanţelor de forţă majoră, precum şi al dificultăţilor tehnice în funcţionarea complexului de mijloace software şi hardware ale băncii centrale de date a SIA RPRAC din vina terţelor persoane, este posibilă suspendarea funcționării Sistemului informaţional cu notificarea ulterioară a participanţilor conectaţi.

33. Revocarea dreptului de acces la banca centrală de date a SIA RPRAC pentru utilizatorii participanţilor se efectuează în una dintre următoarele situaţii:

1) în temeiul cererii (demersului) conducătorului acestuia;

2) la încetarea raporturilor de muncă/de serviciu ale utilizatorului;

3) la intervenirea modificărilor raporturilor de muncă/de serviciu, iar noile atribuţii nu impun accesul la datele din banca centrală de date a SIA RPRAC;

4) la constatarea încălcării de către utilizatorul participantului a măsurilor de securitate informaţională a SIA RPRAC.

34. Lucrările necesare de înlăturare a mijloacelor software de la locul de muncă al participantului sistat se execută în termenul coordonat cu participantul, cu semnarea actului de excludere a acestuia.

VIII. Modalitatea de accesare a SIA RPRAC de către alte organe centrale de specialitate ale administraţiei publice

35. Accesul la informaţia din SIA RPRAC pentru alte organe centrale de specialitate ale administraţiei publice se efectuează în baza acordului încheiat între deţinătorul SIA RPRAC şi organul central de specialitate al administraţiei publice, la solicitarea conducătorului organului.

36. Acordul menţionat la pct. 35 din prezentul Regulament se încheie numai cu organele centrale de specialitate ale administraţiei publice, care, conform legislaţiei în vigoare, au dreptul de a solicita şi de a primi informaţii din SIA RPRAC şi deţin certificatul cheii publice pentru autentificare şi servicii de securitate, emis de Centrul de certificare a cheilor publice al autorităţilor administraţiei publice.

37. Categoriile de informaţii din SIA RPRAC la care se permite accesul organului central de specialitate al administraţiei publice se stabilesc în acordurile încheiate între aceştea. Informaţiile recepţionate în baza acordului nu pot fi transmise persoanelor neautorizate, dacă legislaţia în vigoare sau tratatele internaţionale la care Republica Moldova este parte nu prevede altfel.

IX. Asigurarea protecţiei şi securităţii informaţiei şi resurselor informaţionale ale SIA RPRAC

38. Măsurile de protecţie şi securitate a informaţiei cu privire la persoanele aflate în detenţie în instituţiile penitenciare din SIA RPRAC reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a SIA RPRAC şi se efectuează neîntrerupt de către toţi participanţii.

39. Obiecte ale asigurării protecţiei şi securităţii informaţiei din SIA RPRAC se consideră:

1) masivele informaţionale, indiferent de formele păstrării, bazele de date, suporturile materiale care conţin informaţii de categorie specială cu caracter personal;

2) sistemele informaţionale, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii care asigură activitatea SIA RPRAC;

3) sistemele de telecomunicaţii, reţelele, inclusiv mijloacele de confecţionare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei de categorie specială cu caracter personal.

40. Protecţia informaţiei de categorie specială de date cu caracter personal privind persoanele aflate în detenţie, din SIA RPRAC se efectuează prin următoarele metode:

1) prevenirea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice speciale a datelor din SIA RPRAC transmise prin aceste reţele, asigurată prin folosirea metodelor de cifrare şi criptare a acestei informaţii, inclusiv cu utilizarea măsurilor organizatorice, tehnice şi de regim;

2) excluderea accesului neautorizat la datele de categorie specială cu caracter personal din SIA RPRAC, asigurată prin folosirea mijloacelor speciale tehnice şi de program, cifrarea acestor informaţii, inclusiv prin măsurile organizatorice şi de regim;

3) prevenirea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor de categorie specială cu caracter personal sau defecţiuni în funcţionarea complexului tehnic şi de program, asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizarea sistemului de control al securităţii softului şi efectuarea periodică a copiilor de siguranţă;

4) prevenirea acţiunilor intenţionate şi/sau neintenţionate ale utilizatorilor, care pot conduce la distrugerea sau modificarea datelor din SIA RPRAC.

41. Fiecare participant elaborează, aprobă şi organizează implementarea documentului care stabileşte politica de securitate informaţională pentru asigurarea respectării regulilor, standardelor şi normelor general acceptate în domeniul securităţii informaţionale, cu includerea:

1) identităţii persoanei responsabile de politica de securitate;

2) principalelor măsuri tehnico-organizatorice necesare de asigurare a funcţionării SIA RPRAC;

3) procedurilor interne ce exclud cazurile de modificare neautorizată a mijloacelor software şi/sau a informaţiei de categorie specială de date cu caracter personal din SIA RPRAC;

4) categoriilor resurselor informaţionale ale participantului, cu indicarea nivelului necesar de securitate pentru fiecare categorie;

5) listei nominale a utilizatorilor autorizaţi să acceseze datele din SIA RPRAC;

6) responsabilităţilor personalului participantului privind asigurarea securităţii informaţionale;

7) procedurilor de control intern al participantului privind respectarea condiţiilor de securitate informaţională.

42. Fiecare participant desemnează o persoană subordonată nemijlocit conducătorului instituţiei, responsabilă de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate informaţională.

Persoana responsabilă de politica securităţii informaţionale asigură definirea clară a tuturor responsabilităţilor cu privire la securitatea informaţiei de categorie specială de date cu caracter personal din SIA RPRAC (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele.

43. În cazul operării cu informaţia din SIA RPRAC, ce a devenit cunoscută utilizatorului/ participantului în urma activităţii sale, va fi asigurat regimul de confidenţialitate în modul stabilit de legislaţie şi care presupune următoarele acţiuni:

1) limitarea numărului persoanelor cu drept de acces la datele de categorie specială cu caracter personal din SIA RPRAC;

2) monitorizarea procedurii de admitere şi delimitarea funcţională a responsabilităţilor persoanelor care au acces la informaţia din SIA RPRAC;

3) identificarea şi autentificarea utilizatorilor cu folosirea mijloacelor speciale de autentificare;

4) executarea măsurilor de protecţie a informaţiei de categorie specială de date cu caracter personal în cadrul păstrării, prelucrării şi transmiterii acesteia prin intermediul canalelor de comunicaţii.

X. Controlul şi răspunderea

44. Gestionarea SIA RPRAC este supusă controlului intern şi extern.

Controlul intern privind organizarea şi funcţionarea SIA RPRAC se efectuează de către Departamentul Instituţiilor Penitenciare al Ministerului Justiţiei.

Controlul extern asupra respectării cerinţelor privind crearea, ţinerea, exploatarea şi reorganizarea Registrului se efectuează de către Ministerul Tehnologiei Informaţiei şi Comunicaţiilor.

45. Persoanele cu funcţii de răspundere, în obligaţiile cărora intră gestionarea SIA RPRAC, furnizarea informaţiilor de categorie specială cu caracter personal din SIA RPRAC, precum şi asigurarea funcţionării SIA RPRAC, poartă răspundere personală în conformitate cu legislaţia în vigoare pentru plenitudinea, autenticitatea, veridicitatea, integritatea informaţiilor, precum şi pentru păstrarea şi utilizarea lor.

46. Organul central de specialitate al administraţiei publice competente care are acces la informaţiile din SIA RPRAC, precum şi destinatarul informaţiilor ce conţin date de categorie specială cu caracter personal poartă răspundere conform legislaţiei în vigoare pentru divulgarea, transmiterea acesteia persoanelor neautorizate şi pentru utilizarea ei în alte scopur decît cele stabilite de legislaţie.