GUVERNUL REPUBLICII MOLDOVA

H O T Ă R Î R E

nr. _____ din _____ 2019

cu privire la aprobarea Regulamentul cu privire la organizarea și funcționarea Sistemului informațional automatizat de informare și comunicare privind prevenirea și combaterea spălării banilor

În temeiul art. 19, alin. (1) lit. m) al Legii nr. 308 din 22 decembrie 2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (Monitorul Oficial al Republicii Moldova, 2018, nr.58-66, art. 133), Guvernul Republicii Moldova

HOTĂRĂŞTE:

1. Se aprobă Regulamentul cu privire la organizarea și funcționarea Sistemului informațional automatizat de informare și comunicare privind prevenirea și combaterea spălării banilor (se anexează).

2. Serviciul Prevenirea și Combaterea Spălării Banilor, în calitate de posesor al Sistemului informațional automatizat de informare și comunicare privind combaterea spălării banilor, va asigura implementarea, funcționarea și dezvoltarea SIA ICCSB în conformitate cu legislația în vigoare și acordurile internaționale la care Republica Moldova este parte.

3. Serviciul Tehnologia Informației și Securitate Cibernetică, în calitate de posesor al platformei guvernamentale tehnologice comune (MCloud), va asigura integrarea SIA ICCSB, garantînd accesul la resursele informaţionale de stat, conform normelor de acces reglementate.

4. Realizarea prevederilor prezentei hotărîri se va efectua din contul și în limita mijloacelor financiare prevăzute anual în bugetul de stat și altor mijloace, conform legii.

5. Controlul asupra executării prezentei hotărâri se pune în sarcina Serviciului Prevenirea și Combaterea Spălării Banilor.

Prim-ministru **ION CHICU**

Contrasemnează:

Ministrul finanțelor **SERGHEI PUȘCUȚA**

REGULAMENT

cu privire la organizarea și funcționarea Sistemului Informațional Automatizat de Informare şi Comunicare privind Prevenirea și Combaterea Spălării Banilor

I. DISPOZIȚII GENERALE

1. Regulamentul privind organizarea şi funcţionarea Sistemului informaţional automatizat de informare şi comunicareprivind prevenirea și combaterea spălării banilor (în continuare – Regulament) *este elaborat în conformitate cu prevederile Legii nr.467/2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr.6-12, art.44) și Hotărîrea Guvernului nr.14/2018 cu privire la cu privire la aprobarea Concepţiei tehnice a Sistemului informaţional automatizat de informare şi comunicare privind prevenirea şi combaterea spălării banilor,* și stabileşte modul de organizare şi conţinutul informaţional privind activitățile și tranzacțiile suspecte în ceea ce privește acțiunile de spălare a banilor, infracțiunile asociate acestora şi de finanţare a terorismului, precum și alte informații relevante colectate de Serviciul Prevenirea şi Combaterea Spălării Banilor în conformitate cu prevederile Legii nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, subiecţii raporturilor juridice în domeniul creării şi funcţionării Sistemului informațional automatizat de informare şi comunicare privind prevenirea și combaterea spălării banilor (în continuare – SIA ICCSB), drepturile şi obligaţiile acestora, obiectele informaţionale şi lista datelor incluse în acestea, procedurile de colectare și gestiune a datelor, accesul la datele SIA ICCSB, interoperabilitatea cu alte registre şi sisteme informaţionale, modalitatea de ţinere şi asigurare a funcţionării SIA ICCSB, formele de exercitare a controlului şi atragere la răspundere.

2. În sensul prezentului Regulament următoarele noţiuni semnifică:

analiză bazată pe risc – componentă tehnologică a SIA ICCSB, care permite obținerea informațiilor cu risc sporit conform criteriilor stabilite în momentul desfășurării, identificării sau recepționării acestora;

entități raportoare – persoane fizice și juridice obligate în conformitate cu prevederile Legii nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și a finanțării terorismului să furnizeze informații către SIA ICCSB în scopul prevenirii spălării banilor și finanțării terorismului;

formular special – totalitatea informațiilor structurate destinate informării Serviciului Prevenirea şi Combaterea Spălării Banilor cu privire la bunurile suspecte, activităţile sau tranzacţiile suspecte de spălare a banilor, de infracţiuni asociate acestora şi de finanţare a terorismului.

Grupul EGMONT – organizaţie internaţională a Unităţilor de Inteligenţă Financiară, care asigură cadrul de eficientizare a cooperării privind schimbul de informaţii, instruire, schimb de experienţă şi de know-how în domeniul prevenirii şi combaterii spălării banilor şi a finanţării terorismului.

prelucrare automatizată de date – orice operaţiune sau serie de operaţiuni care se efectuează asupra datelor prin mijloace automatizate, precum: colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;

raport statistic – document generat de către SIA ICCSB, care reflectă sinteza datelor stocate în sistem;

registrator – entitățile raportoare specificate în art.4 din Legea 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;

resursă analitică de informare – totalitatea informațiilor colectate și prelucrate de Serviciul Prevenirea şi Combaterea Spălării Banilor stocate în bazele de date SIA ICCSB;

sistem informațional automatizat de informare şi comunicare privind prevenirea și combaterea spălării banilor – sistem informaţional automatizat constituit dintr-un ansamblu de resurse şi tehnologii informaţionale, mijloace tehnice de program şi metodologii aflate în interconexiune şi care este destinat pentru recepționarea, stocarea, prelucrarea, informarea, analiza, prevenirea și diseminare informaţiilor cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;

utilizator – persoană mandatată cu drept de acces, deplin sau partajat, asupra informaţiei din resursa informaţională;

II. SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII, EXPLORĂRII ȘI UTILIZĂRII SIA ICCSB, ATRIBUȚIILE ACESTORA

3. Subiecții în domeniul creării, exploatării și al utilizării conținutului SIA ICCSB sunt:

1) proprietarul;
2) posesorul;
3) registratorul;
4) furnizorul;
5) destinatarul;
6) utilizatorul.

4. Proprietarul SIA ICCSB este statul care realizează dreptul de proprietate, de gestionare şi utilizare datelor din acesta.

5. Posesorul SIA ICCSB este Serviciul Prevenirea și Combaterea Spălării Banilor.

6. Deținătorul SIA ICCSB este Serviciul Prevenirea și Combaterea Spălării Banilor cu drept de creare, gestionare, utilizare şi deţinere a resursei informaţionale, având atribuţia de asigurare a condiţiilor juridice, organizatorice şi financiare, îndeplinind atît atribuţiile de posesor cît și cele stabilite de lege, după cum urmează:

1) asigură condiţiile organizatorice şi financiare pentru funcţionarea SIA ICCSB;
2) stabileşte scopurile şi sarcinile funcţionale ale SIA ICCSB;
3) determină obiectele informaţionale supuse înregistrării în SIA ICCSB şi conţinutul acestora;
4) monitorizează procesul de înregistrare şi prelucrare a datelor în SIA ICCSB;
5) gestionează activitatea de exploatare şi ţinere a conţinutului informaţional al SIA ICCSB;
6) asigură securitatea şi protecţia datelor din SIA ICCSB;
7) aprobă şi execută modificări/rectificări privind ajustările necesare pentru funcţionarea normală și *actuală* a SIA ICCSB;
8) autorizează, suspendă şi revocă dreptul de acces în SIA ICCSB;
9) stabileşte măsurile tehnice şi organizatorice de protecţie şi securitate a SIA ICCSB;
10) monitorizează şi, după caz, ajustează cerinţele de securitate şi conformitate a SIA ICCSB la domeniul protecţiei datelor cu caracter personal;
11) exercită alte atribuţii necesare asigurării bunei funcţionări a SIA ICCSB.

7. Drepturile şi obligaţiile deținătorului sunt stabilite în conformitate cu Legea nr.467/2003 cu privire la informatizare şi la resursele informaţionale de stat şi Legea nr.308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

8. Registratori sînt entitățile raportoare specificate în art.4 din Legea 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, care, după caz, prin intermediul angajaţilor acestora împuterniciţi cu atribuţii de acces în sistem, în baza atribuţiilor acordate prin lege, regulamente, specificaţiile din statul de personal al entităților raportoare, profilului de acces al resursei informaţionale.

9. În calitate de registratori, entitățile raportoare au următoarele atribuţii:

1) asigură colectarea, introducerea şi prelucrarea informaţiei relevante în baza de date a SIA ICCSB, în termenele şi condiţiile stabilite;
2) asigură autenticitatea, plenitudinea, integritatea datelor din SIA ICCSB;
3) asigură securitatea şi confidenţialitatea informaţiei introduse în SIA ICCSB ;
4) asigură introducerea şi prelucrarea datelor şi monitorizează procesul de introducere a acestora;
5) raportează de fiecare dată deținătorului incidentele de infrastructură, erorile de sistem sau erorile cauzate de factorul uman în scopul remedierii acestora;
6) solicită deținătorului autorizarea accesului, precum şi suspendarea şi revocarea drepturilor de acces în SIA ICCSB;

7) adresează deținătorului cereri de modificare a drepturilor de acces/rolurilor unor utilizatori;

8) raportează deținătorului problemele de sistem în utilizarea SIA ICCSB;

9) înaintează demersuri privind necesitatea de dezvoltare şi îmbunătăţire a SIA ICCSB;

10) participă în grupurile de lucru organizate în scopul dezvoltării şi îmbunătăţirii SIA ICCSB.

10. În cazul în care registratorii sunt persoane juridice acestia desemnează şi informează posesorul despre numărul, numele, prenumele angajaţilor acestora cu atribuţii de introducere nemijlocită a datelor în baza de date şi împuterniciri specifice ce sînt delegate în sensul îndeplinirii atribuţiilor legate de gestionare în SIA ICCSB.

11. Fiecare registrator, după caz, trebuie să prevadă în statul de personal o funcţie responsabilă de introducerea datelor în SIA ICCSB. Numele, prenumele şi datele de contact ale persoanelor angajate în aceste funcţii, precum şi orice modificări cu privire la datele acestora se comunică deținătorului.

12. Furnizorii de date către SIA ICCSB sunt:

1) Persoana fizică sau persoana juridică de drept privat sau public, care prezintă registratorului, în format electronic, date despre obiectul SIA ICCSB;

2) Serviciile competente din alte țări (jurisdicții) și organizațiile internaționale de specialitate.

13. Furnizorul:

1) asigură corectitudinea şi autenticitatea datelor introduse sau prezentate pentru a fi introduse în SIA ICCSB;

2) asigură confidenţialitatea datelor;

3) raportează posesorului problemele de funcţionalitate ale SIA ICCSB.

14. Destinatarii datelor SIA ICCSB sunt:

1) organele de drept, judiciare și alte autorități competente, care primesc informații privind activitățile și tranzacțiile suspectate de spălare a banilor, infracțiuni conexe și finanțare a terorismului de la entitățile raportoare, precum și alte informații relevante colectate în conformitate cu prevederile Legii nr. 308/2017 privind prevenirea și combaterea spălării banilor și finanțării terorismului;

2) entitățile raportoare care primesc informații privind modul de raportare și corectitudinea introducerii datelor în SIA ICCSB;

3) autoritățile cu funcții de supraveghere a entităților raportoare și alte autorități competente, care primesc informații cu privire la riscurile aferente spălării banilor și finanțării terorismului, noile tendințe și tipologii în domeniul spălării banilor și finanțării terorismului, încălcările stabilite în domeniile de competență și lacunele în actele normative în partea ce ține de prevenirea riscurilor de spălare a banilor și de finanțare a terorismului;

4) autoritățile competente din alte țări (jurisdicții), precum și organizațiile internaționale în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului în conformitate cu prevederile Legii nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

15. Destinatarul este persoana fizică sau juridică de drept privat sau public care este în drept, potrivit legislaţiei, de a avea acces la informaţii cu accesibilitate limitată. Drepturile şi obligaţiile solicitantului informaţiei din SIA ICCSB se stabilesc în conformitate cu legislaţia privind accesul la informaţie, legislaţia privind protecţia datelor cu caracter personal, Legea 308/2017 cu privire la prevenirea și combaterea spălării banilor şi prezentul Regulament.

16. Utilizatorul este persoana fizică sau juridică de drept privat sau public împuternicită, potrivit legislaţiei, cu drept de acces deplin sau partajat, public sau intern în SIA ICCSB.

17. Utilizatorul poate raporta deținătorului problemele ce ţin de accesarea informaţiei conţinute în SIA ICCSB.

18. Utilizatorul:

1) asigură securitatea şi confidenţialitatea informaţiei vizualizate sau prelucrate în SIA ICCSB;

2) utilizează datele din SIA ICCSB conform scopului şi destinaţiei acestora.

III. STRUCTURA ŞI FUNCŢIILE SIA ICCSB

19. Funcţiile de bază ale SIA ICCSB sunt:

1) formarea unei resurse analitico-informaţionale departamentale a Serviciului Prevenirea şi Combaterea Spălării Banilor;

2) stabilirea unui sistem eficient de schimb de informaţii dintre Serviciul Prevenirea şi Combaterea Spălării Banilor şi entităţile raportoare, organele cu funcţii de supraveghere a entităţilor raportoare, organele de drept, judiciare şi alte autorităţi competente la nivel naţional şi internaţional;

3) crearea unui sistem de obţinere rapidă a informaţiilor necesare pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului din toate sursele posibile, la nivel naţional şi internaţional;

4) procesarea promptă a informaţiilor privind relaţiile financiare şi economice necesare prevenirii şi combaterii spălării banilor şi finanţării terorismului;

5) organizarea circulaţiei documentelor şi păstrarea evidenţei Serviciului Prevenirea şi Spălarea Banilor;

6) organizarea funcţionării circuitului analitic şi statistic care asigură analiza informaţiilor şi evaluează riscurile de spălare a banilor şi finanţare a terorismului;

7) organizarea suportului informaţional şi informarea persoanelor şi organizaţiilor conform competenţei lor în legătură cu prevenirea şi combaterea spălării banilor;

8) asigurarea securităţii şi protecţiei informaţiilor care se desfăşoară la toate etapele de acumulare, stocare şi utilizare a resurselor informaţionale guvernamentale care se referă la funcţionarea SIA ICCSB;

9) asigurarea calităţii informaţiilor prin crearea şi menţinerea componentelor sistemului de calitate, bazat pe abordarea procedurală.

20. Spaţiul funcţional al SIA ICCSB reprezintă o totalitate de funcţii realizate de subsisteme automatizate şi/sau automate separate, care interacţionează între ele.

21. În cadrul funcţionării SIA ICCSB se realizează următoarele funcţii specifice ale sistemului, grupate în circuite funcţionale speciale:

1) Circuitul funcţional "Informarea privind activităţi sau tranzacţii şi schimbul de informaţii cu serviciile competente ale altor ţări (jurisdicţii) şi cu organizaţiile internaţional de specialitate" (**e-Informare**) este un subsistem de interacţiune cu entităţile raportoare şi cu organizaţiile internaţionale de specialitate şi alte organizaţii competente, ce include următoarele funcţii:

a) primirea, înregistrarea şi procesarea informaţiei parvenite la Serviciul Prevenirea şi Combaterea Spălării Banilor de la entităţile raportoare cu privire la o proprietate dubioasă, activităţi sau tranzacţii care sînt suspecte de spălare a banilor, infracţiuni asociate acestora şi de finanţare a terorismului;

b) gestionarea formularelor speciale;

c) gestionarea mecanismului asincron de informare bazat pe evenimente, care permite entităţilor raportoare să se conecteze la SIA ICCSB şi să transmită informaţiile necesare în timp real;

d) schimbul de informaţii dintre Serviciul Prevenirea şi Combaterea Spălării Banilor şi entităţile raportoare în vederea obţinerii datelor sau informaţiilor suplimentare necesare;

e) crearea şi gestionarea subsistemului de schimb internaţional de informaţii;

f) primirea, înregistrarea şi procesarea informaţiei parvenite la Serviciul Prevenirea şi Combaterea Spălării Banilor de la organizaţiile internaţionale despre activităţile şi tranzacţiile suspecte de spălare a banilor, infracţiunile asociate acestora şi de finanţare a terorismului;

g) furnizarea de informaţii organizaţiilor internaţionale în ceea ce priveşte activităţile şi tranzacţiile suspecte de spălare a banilor, infracţiunile asociate acestora şi de finanţare a terorismului;

h) schimbul de informaţii dintre Serviciul Prevenirea şi Combaterea Spălării Banilor şi organizaţiile internaţionale pentru a obţine informaţii sau date suplimentare necesare;

2) Circuitul funcţional “Asigurarea interacţiunii informaţionale cu resursele informaţionale guvernamentale, departamentale şi teritoriale”(**AMLOP**) este un subsistem care permite Serviciului Prevenirea şi Combaterea Spălării Banilor să obţină de la autorităţile publice informaţiile necesare, inclusiv accesul online la resursele informaţionale (inclusiv informaţii, ce conţin date cu caracter personal), ce include următoarele funcţii:

a) interacţiunea SIA ICCSB cu resursele informaţionale externe indicate la pct.4 subpct. 2) lit.d) prin intermediul platformei de interoperabilitate (MConnect);

b) crearea şi gestionarea mecanismului flexibil de autentificare şi de control al accesului utilizatorilor SIA ICCSB în sistemele informaţionale de stat, utilizînd serviciul electronic guvernamental de autentificare şi control al accesului (MPass);

c) asigurarea unui mecanism flexibil şi sigur de protocolare şi audit, care să garanteze evidenţa evenimentelor în contextul utilizării sistemelor şi resurselor informaţionale guvernamentale atît ca mecanisme interne tehnologice SIA ICCSB, cît şi cu ajutorul serviciului electronic guvernamental de jurnalizare (MLog);

3) Circuitul funcţional “Analitica şi Supraveghere” (**AMLAS**) reprezintă un sistem informaţional modular de producere, care asigură efectuarea analizei informaţiei, inclusiv prelucrarea şi analiza datelor statistice, evaluarea riscurilor, precum şi funcţii de supraveghere în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului ce include următoarele:

a) desfăşurarea analizei operaţionale – studierea continuă a informaţiilor parvenite de la entităţile raportoare, precum şi din orice alte surse de informaţii în vederea identificării anumitor cazuri suspecte în ceea ce priveşte spălarea banilor şi finanţarea terorismului, în funcţie de tipul tranzacției şi suma primită;

b) asigurarea analizei automatizate şi automate inteligente, bazată pe evenimente, a informaţiei primite şi stocate în baza de date;

c) desfăşurarea unei analize strategice bazate pe evaluarea generală a tendinţelor pe termen mediu şi lung, precum şi a previziunilor şi estimărilor destinate să justifice deciziile strategice şi de management pentru a preveni şi a combate spălarea banilor şi finanţarea terorismului;

d) evaluarea riscurilor de spălare a banilor şi de finanţare a terorismului;

e) desfăşurarea analizei materialului statistic şi evaluarea eficienţei sistemului de prevenire şi combatere a spălării banilor şi finanţării terorismului;

f) identificarea informaţiei necesare pentru desfăşurarea activităţii de supraveghere a Serviciului Prevenirea şi Combaterea Spălării Banilor;

g) pregătirea documentelor necesare legate de activitatea de supraveghere a Serviciului Prevenirea şi Combaterea Spălării Banilor, în conformitate cu competenţele sale;

h) gestionarea deciziilor de sancţionare;

i) gestionarea informaţiei legate de activitatea de supraveghere, informarea autorităţilor de supraveghere;

4) Circuitul funcţional “Evidenţa electronică a investigaţiilor financiare, notificarea, informarea şi transmiterea informaţiei” (**e-Case**) presupune un sistem informaţional modular de producere care asigură punerea în aplicare şi desfăşurarea investigaţiilor financiare pentru a stabili sursa de proprietate suspectă precum şi pregătirea şi transmiterea informaţiei în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului către organizaţiile competente interesate, organele de drept, entităţile raportoare, organizaţiile internaţionale competente, precum şi altă informaţie corespunzătoare colectată de Serviciul Prevenirea şi Combaterea Spălării Banilor în conformitate cu competenţele sale, ce include următoarele funcţii:

a) evidenţa şi prelucrarea informaţiilor primite, a documentelor analitice şi a altor documente;

b) formarea, evidenţa şi procesarea documentelor administrative interne, informative şi analitice, formarea şi gestionarea fluxurilor interne de informaţii;

c) selecţia automatizată, precum şi automată, inteligentă, bazată pe evenimente, a informaţiilor primite şi stocate în baza de date şi formarea documentelor analitice pe baza acestora;

d) asigurarea activităţii de informare a angajaţilor Serviciului Prevenirea şi Combaterea Spălării Banilor în timpul desfăşurării investigaţiei financiare, precum şi la îndeplinirea altor atribuţii de serviciu;

e) pregătirea şi distribuirea, inclusiv în mod automatizat şi/sau automat, autorităţilor competente a informaţiei prezentate de entităţile raportoare privind activităţile şi tranzacţiile suspecte de spălare a banilor, infracţiunile asociate acestora şi de finanţare a terorismului, precum şi altă informaţie corespunzătoare colectată în conformitate cu Legea nr.308/2017 privind prevenirea şi combaterea spălării banilor şi finanţării terorismului;

f) asigurarea informării automatizate şi automate a autorităţilor competente şi a organelor de drept imediat după apariţia unor suspiciuni justificate de spălare a banilor, de finanţare a terorismului, inclusiv prin transmiterea informaţiilor în sistemul informaţional al organelor de drept sau al altor organizaţii competente;

g) asigurarea notificării automatizate şi automate a entităţilor raportoare, a organelor cu funcţii de supraveghere şi altor autorităţi competente cu privire la aspectele legate de prevenirea şi combaterea spălării banilor şi finanţării terorismului;

h) furnizarea informaţiei în regim automatizat şi automat organelor naţionale, organelor şi instituţiilor altor ţări (jurisdicţii), precum şi organizaţiilor internaţionale în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului.

IV. SPAȚIUL INFORMAȚIONAL, OBIECTELE INFORMAȚIONALE ALE SIA ICCSB

22. Datele conţinute în SIA ICCSB se elaborează şi se clasifică conform prevederilor actelor legislative în vigoare, regulamentelor şi standardelor aprobate, specificaţiei tehnice a resurselor şi sistemelor informaţionale utilizate în contextul gestionării automatizate a dosarelor.

23. Documentele de bază utilizate în ICCSB sunt:

1) Documente de bază:

a) documente de intrare înregistrate în SIA ICCSB referitor la activităţile şi tranzacţiile suspecte de spălare a banilor, infracţiunile asociate acestora şi de finanţare a terorismului;

b) materiale şi informaţii documentate privind prevenirea şi combaterea spălării banilor şi finanţării terorismului;

c) formular special de la entităţile raportoare;

d) referinţe analitice;

e) raport privind investigaţia financiară;

f) cereri adresate autorităţilor competente, forţelor de ordine şi organelor cu funcţii de supraveghere, organizaţiilor naţionale şi entităţilor raportoare;

g) cereri adresate organizaţiilor internaţionale;

h) răspunsurile la cererile organizaţiilor internaţionale;

i) documente referitoare la blocarea tranzacţiilor cu bunuri;

j) solicitări şi permisiuni de divulgare şi transfer de informaţii;

k) documente de informare şi referinţă;

l) documente de informare;

m) rapoartele finale;

n) raport de analiză strategică;

o) documente analitice şi statistice;

p) documente referitoare la evaluarea riscurilor;

q) documente referitoare la activităţi de supraveghere;

r) decizii de sancţionare;

s) documente şi materiale cu caracter informativ emise de către Serviciul Prevenirea şi Combaterea Spălării Banilor;

2) Documente tehnologice de bază în SIA ICCSB:

a) documente administrative, de reglementare, procedurale şi tehnologice;

b) profilurile utilizatorilor;

c) înregistrarea fişierelor – registru cu privire la acţiuni, solicitări şi interacţiunea utilizatorilor cu SIA ICCSB;

d) certificate electronice de utilizator şi alte informaţii de documentare a utilizatorilor.

24. Obiectele informaţionale de bază ale SIA ICCSB sînt:

1) notă analitică;

2) raport de investigaţie financiară;

3) diseminare de materiale şi informaţii;
4) răspuns la diseminarea de materiale şi informaţii;
5) solicitări adresate entităţilor raportoare;
6) răspuns de la entităţile raportoare;
7) solicitare Grup EGMONT ieşire;
8) răspuns Grup EGMONT ieşire;
9) solicitare Grup EGMONT intrare;
10) răspuns Grup EGMONT intrare;
11) decizie de sistare;
12) decizie de anulare a sistării;
13) solicitare permisiune de diseminare ieşire;
14) răspuns permisiune de diseminare intrare;
15) solicitare de permisiune de diseminare intrare;
16) răspuns permisiune de diseminare ieşire;
17) informare generală;
18) raport final;
19) raport de iniţiere a analizei strategice;
20) raport de supraveghere a conformităţii;
21) decizie de sancţionare.

25. Identificarea obiectelor informaţionale

1) Identificatorul obiectului informaţional "Nota analitică", este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

2) identificatorul obiectului informaţional "Raport Investigaţie Financiară" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

3) identificatorul obiectului informaţional "Diseminarea de materiale şi informaţii" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

4) identificatorul obiectului informaţional "Răspuns la Diseminarea de materiale şi informaţii" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

5) identificatorul obiectului informaţional "Solicitări la entităţi raportoare" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

6) identificatorul obiectului informaţional "Răspuns de la entităţi raportoare" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

7) identificatorul obiectului informaţional "Solicitare EGMONT ieşire" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

8) identificatorul obiectului informaţional "Răspuns EGMONT ieşire" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

9) identificatorul obiectului informaţional "Solicitare EGMONT intrare" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

10) identificatorul obiectului informaţional "Răspuns EGMONT intrare" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

11) identificatorul obiectului informaţional "Decizie de sistare" este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

12) identificatorul obiectului informaţional “Decizia de anulare a sistării” este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

13) identificatorul obiectului informaţional “Solicitare de permisiune de diseminare ieşire” este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

14) identificatorul obiectului informaţional “Răspuns permisiune de diseminare intrare” este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

15) identificatorul obiectului informaţional “Solicitare adresată Serviciului Prevenirea şi Combaterea Spălării Banilor pentru permisiunea de a dezvălui şi a transmite informaţii (Solicitare de permisiune de diseminare intrare)” este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

16) identificatorul obiectului informaţional “Răspunsul Serviciului Prevenirea şi Combaterea Spălării Banilor la cererea de permisiune de divulgare şi transfer de informaţii (Răspuns Permisiune de diseminare ieşire)” este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

17) identificatorul obiectului informaţional “Informarea autorităţilor de supraveghere competente şi a entităţilor raportoare (Informare generală)” este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

18) identificatorul obiectului informaţional “Raport final” este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

19) identificatorul obiectului informaţional “Raport de iniţiere a analizei strategice” este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

20) identificatorul obiectului informaţional “Raport asupra rezultatelor supravegherii (Raport supraveghere conformitate este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

21) identificatorul obiectului informaţional “Decizie de sancţionare este constituit dintr-un număr generat de e-Case format din codul unic al obiectului, un număr de ordine atribuit de e-Case automat şi anul şi ziua înregistrării;

26. Scenariile de bază sunt:

1) primirea informaţiei de la entităţile raportoare:

a) pregătirea unui formular special;

b) completarea de către entităţile raportoare a unui formular special şi transmiterea acestuia prin intermediul subsistemului e-Informare, în format electronic, în adresa Serviciului Prevenirea şi Combaterea Spălării Banilor, în conformitate cu procedura stabilită;

c) verificarea şi introducerea datelor în baza de date SIA ICCSB;

d) oferirea unui API specializat (Application Programming Interface – interfaţa software a unei aplicaţii de integrare specializată) entităţilor raportoare;

e) integrarea pe partea e-Informare a SIA ICCSB a entităţilor raportoare a subsistemului de acumulare de informaţii;

f) primirea informaţiilor din sistemele şi registrele informaţionale de stat, departamentale şi teritoriale.

2) obţinerea datelor din sistemele informaţionale automatizate utilizînd AMLOP:

a) resursele informaţionale automatizate conform pct.41;

b) alte sisteme informaţionale automatizate ale autorităţilor publice naţionale şi organelor cu funcţii de supraveghere a entităţilor raportoare – oferă acces la informaţii în conformitate cu prevederile Legii nr.308/2017 privind prevenirea şi combaterea spălării banilor şi finanţării terorismului.

3) primirea informaţiei de la autorităţile competente din ţară, precum şi de la autorităţile competente din alte ţări (jurisdicţii) şi organizaţiile internaţionale specializate, procesarea documentelor primite prin intermediul subsistemului e-Case:

a) primirea informaţiilor sub formă de documente de intrare;
b) introducerea documentelor în SIA ICCSB prin intermediul subsistemului e-Case;
c) analiza şi executarea documentelor;
d) verificarea datelor şi dacă este necesar, introducerea datelor în baza de date SIA ICCSB.
e) primirea informaţiilor din alte surse;

4) proces analitic operaţional:

a) analiza informaţiilor, automat/automatizat prin intermediul subsistemului AMLAS, recepţionate de la registratori precum şi informaţiile furnizate de autorităţile competente din ţară, autorităţile competente din alte ţări (jurisdicţii) şi organizaţiile internaţionale specializate, acumulate în baza de date SIA ICCSB;
b) analiza informaţiilor primite din orice sursă posibilă;
c) generarea automată a proiectului de referinţă analitică, pe baza unei analize automatizate, şi cazurile identificate prin criterii care ar putea fi suspecte în sensul spălării banilor şi finanţării terorismului, precum şi notificarea angajatului Serviciului Prevenirea şi Combaterea Spălării Banilor;
d) monitorizarea financiară;
e) crearea unui raport privind investigaţia financiară (RIF) şi efectuarea unei investigaţii financiare;

5) procesele de analiză strategică;

a) crearea unui raport privind iniţierea analizei strategice (Raport de iniţiere a analizei strategice);
b) analiza informaţiilor primite şi acumulate;
c) pregătirea documentelor şi rapoartelor analitice şi statistice.

6) procesul de supraveghere;

a) primirea şi analizarea informaţiilor din baza de date, precum şi alte documente ale SIA ICCSB;
b) pregătirea în sistem a raportului cu privire la rezultatele supravegherii;
c) luarea deciziei de sancţionare, pregătirea în SIA ICCSB a deciziei de sancţionare;
d) informarea autorităţilor de supraveghere.

7) pregătirea şi furnizarea de informaţii:

a) pregătirea şi transmiterea către autorităţile competente a informaţiilor prezentate de către entităţile raportoare despre activităţile şi tranzacţiile suspecte în sensul spălării banilor, legate de infracţiuni şi finanţarea terorismului, precum şi alte informaţii relevante, colectate în conformitate cu Legea nr.308/2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului;
b) pregătirea şi transmiterea informaţiilor către autorităţile competente privind apariţia unor suspiciuni justificate de spălare a banilor şi/sau finanţare a terorismului;
c) pregătirea documentelor şi notificarea entităţilor raportoare, organelor cu funcţii de supraveghere a entităţilor raportoare şi altor autorităţi competente în problemele ce ţin de prevenirea şi combaterea spălării banilor şi/sau finanţării terorismului;
d) pregătirea documentelor şi transmiterea informaţiilor autorităţilor competente din ţară, precum şi autorităţilor competente din alte ţări (jurisdicţii), organizaţiilor internaţionale în domeniul prevenirii şi combaterii spălării banilor şi/sau finanţării terorismului;
e) utilizarea subsistemului e-Informare pentru informarea entităţilor raportoare, organele de drept şi alte autorităţi competente, organizaţiile naţionale, imediat după apariţia unor suspiciuni justificate de spălare a banilor, finanţare a terorismului, care necesită o luare de atitudine promptă;
f) furnizarea informaţiilor în regim automat (inclusiv pregătirea şi transmiterea informaţiilor prin e-mail) aparţinînd altor ţări (jurisdicţiilor) organelor de drept şi autorităţilor competente, precum şi organizaţiilor internaţionale în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului.

V. REGIM JURIDIC DE UTILIZARE A DATELOR DIN SIA ICCSB

27. Utilizatorii beneficiază de drepturi de acces la informaţia din SIA ICCSB conform atribuţiilor şi funcţiilor deţinute şi regimul juridic al informaţiei accesate. Nivelul de acces la informaţie pentru fiecare participant corespunde funcţiei de serviciu şi/sau profilului de acces.

28. Accesul la resursele informaţionale ale SIA ICCSB este segmentat pentru utilizatorii interni ai SIA ICCSB şi utilizatorii externi.

29. Utilizatori interni ai SIA ICCSB sunt posesorul și deținătorul.

30. Deţinătorul are acces deplin la datele din SIA ICCSB, în scopul prestării serviciilor de administrare, inclusiv mentenanţă adaptivă şi perfectivă a SIA ICCSB .

31. Utilizatori externi ai SIA ICCSB sunt furnizorii, registratorii precum și destinatarii cu drept de acces în temeiul legii.

32. Se interzice utilizarea datelor din SIA ICCSB în scopuri contrare legii.

33. Datele recepţionate din SIA ICCSB nu pot fi transmise persoanelor terţe, dacă legislaţia în vigoare sau tratatele internaţionale la care Republica Moldova este parte nu prevăd altfel.

34. Accesul la datele din SIA ICCSB este condiţionat de rolul utilizatorului. Astfel, registratorul are acces tehnic la datele din SIA ICCSB, ceea ce presupune introducerea datelor. Restul utilizatorilor externi au acces informaţional la datele din SIA ICCSB, ceea ce presupune vizualizarea datelor numai în formatul individual permis pentru fiecare utilizator în parte.

35. Destinatarul datelor din SIA ICCSB nu este în drept să modifice datele obţinute, iar la utilizarea acestora este obligat să indice sursa.

36. Dreptul de acces la SIA ICCSB nu este unul permanent, acesta poate fi suspendat sau revocat în circumstanţele prevăzute în pct.37. Introducerea şi/sau modificarea datelor în SIA ICCSB de pe un nume sau profil de utilizator străin este strict interzisă, urmînd a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure de faptul că profilul de utilizator, precum şi semnătura electronică sînt confidenţiale.

37. Revocarea dreptului de acces la SIA ICCSB se efectuează la cererea/demersul registratorului către posesor, în una dintre următoarele situaţii:

1) la încetarea/suspendarea raporturilor de serviciu/ de muncă ale utilizatorului;
2) la intervenirea modificărilor raporturilor de serviciu/de muncă cînd noile atribuţii nu impun accesul la datele din SIA ICCSB;
3) la constatarea de către posesor a încălcării securităţii informaţionale;
4) în alte cazuri, în limitele prevederilor legislaţiei.

38. Lucrările profilactice planificate în complexul de mijloace software şi hardware se efectuează după notificarea, în scris sau prin e-mail, a registratorilor de către posesor, în baza planului coordonat cu deţinătorul tehnic cu cel puţin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea utilizatorilor şi coordonarea prealabilă cu posesorul în situaţia nefuncţionării sau funcţionării necorespunzătoare a complexului de mijloace software şi hardware.

39. Datele recepţionate din SIA ICCSB nu pot fi transmise persoanelor terţe, fără acordul prealabil al Serviciului Prevenirea și Combaterea Spălării Banilor dacă legislaţia în vigoare sau tratatele internaţionale la care Republica Moldova este parte nu prevăd altfel.

VI. INTEROPERABILITATEA CU ALTE SISTEME INFORMAȚIONALE

40. Pentru asigurarea analizei operative şi automate a conţinutului informaţional al SIA ICCSB cu informaţie veridică, poate fi efectuată interacţiunea şi sincronizarea datelor cu alte sisteme informaţionale inclusiv prin intermediul Platformei Guvernamentale de Interoperabilitate MConnect, importîndu-se automat date spre verificare şi/sau completare a conţinutului informaţional al SIA ICCSB.

41. SIA ICCSB asigură interacţiunea şi schimbul de date cu următoarele resurse informaţionale automatizate:

1) Sistemul informaţional automatizat "Registrul de stat al populaţiei";
2) Sistemul informaţional automatizat "Registrul de stat al unităţilor de drept";
3) Sistemul Informaţional Geografic Naţional, inclusiv Cadastrul bunurilor imobile;
4) Sistemul informaţional automatizat "Registrul de stat transporturilor";
5) Sistemul informaţional al Serviciului Fiscal de Stat;
6) Sistemul informaţional integrat al Poliţiei de Frontieră;
7) Sistemul informaţional integrat vamal
8) Sistemul informaţional automatizat "Registrul informaţiei criminalistice şi criminologice";
9) Sistemul informaţional automatizat "Registrul de evidenţă a contravenţiilor";
10) Evidenta antecedentelor penale cazier MAI
11) Evidenta infracțiunilor si a cauzelor penale MAI
12) Evidenta dosarelor contravenționale si penalităților PR
13) Evidenta accidentelor rutiere
14) Administrația Națională a Penitenciarelor
15) Sistemul informaţional automatizat "Registrul persoanelor reţinute, arestate si condamnate";
16) Sistemul informaţional automatizat "Urmărirea penală: E-Dosar"
17) Sistemului informațional automatizat de gestionare și eliberare a actelor permisive
18) alte sisteme informaţionale automatizate, considerate necesare pentru implementarea şi dezvoltarea SIA ICCSB.

42. SIA ICCSB utilizează următoarele servicii electronice guvernamentale de platformă:

1) serviciul electronic guvernamental de autentificare și control al accesului (MPass), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), aprobat prin Hotărârea Guvernului nr.1090/2013;
2) serviciul electronic guvernamental integrat de semnătură electronică (MSign), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental integrat de semnătură electronică (MSign), aprobat prin Hotărârea Guvernului nr.405/2014;
3) serviciul electronic guvernamental de jurnalizare (MLog), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental de jurnalizare (MLog), aprobat prin Hotărârea Guvernului nr.708/2014.

VII. SECURITATEA ȘI INTEGRITATEA INFORMAȚIEI DIN SIA ICCSB

43. Măsurile de protecţie şi securitate a datelor din SIA ICCSB reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a SIA ICCSB şi se actualizează de către toţi subiecţii SIA ICCSB.

44. Obiecte ale asigurării protecţiei şi securităţii datelor din SIA ICCSB se consideră tot complexul de mijloace software şi hardware care asigură realizarea proceselor informaţionale:

1) baza de date, sistemele informaţionale, sistemele operaţionale, sistemele de gestiune a bazelor de date, sistemele de evidenţă şi alte aplicaţii care asigură funcţionarea SIA ICCSB;
2) sistemele de telecomunicaţii, reţelele, serverele, calculatoarele şi alte mijloace tehnice de prelucrare a datelor.

45. Protecţia datelor din SIA ICCSB se efectuează prin următoarele metode:

1) prevenirea acţiunilor intenţionate şi/sau neintenţionate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor;

2) excluderea accesului neautorizat la datele din SIA ICCSB, asigurată prin folosirea mijloacelor speciale tehnice şi de program;

3) prevenirea distrugerii, modificării datelor sau a defecţiunilor în funcţionarea complexului tehnic şi de program, prin folosirea mijloacelor de protecţie speciale, inclusiv a programelor antivirus prin organizarea sistemului de control al securităţii softului şi efectuarea periodică a copiilor de siguranţă;

4) monitorizarea procesului de exploatare al SIA ICCSB prin intermediul mecanismului de jurnalizare efectuat de deţinătorul acestuia.

46. În procesul de funcționare a SIA ICCSB se va asigura securitatea datelor cu caracter personal, în conformitate cu Legea nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal

47. Schimbul informaţional se efectuează cu utilizarea mijloacelor software şi hardware, doar prin canale securizate, asigurînd integritatea şi securitatea datelor.

48. Utilizatorii interni desemnează o persoană subordonată nemijlocit conducătorului instituţiei, responsabilă de implementarea şi monitorizarea respectării prevederilor normelor de securitate informaţională.

49. Normele de securitate informaţională se aduc la cunoştinţa fiecărui utilizator intern şi se semnează de acesta. Fiecare utilizator intern este obligat să cunoască normele securităţii informaţionale, procedurile pe care trebuie să le respecte în strictă concordanţă cu politica de securitate.

50. Utilizatorii interni asigură instruirea angajaţilor privind metodele şi procedeele de contracarare a pericolelor informaţionale.

VII. CONTROLUL ȘI RESPONSABILITATEA

51. Deținătorul SIA ICCSB este obligat să prevină accesul nesancţionat la datele din acesta, utilizarea ilegală, difuzarea, modificarea sau nimicirea lor.

52. Pentru asigurarea funcţionării eficiente şi neîntrerupte a SIA ICCSB, accesul la date este asigurat continuu.

53. SIA ICCSB se înregistrează în Registrul resurselor şi sistemelor informaţionale de stat şi în Registrul de evidenţă a operatorilor de date cu caracter personal.

54. Responsabilitatea pentru organizarea funcţionării SIA ICCSB aparţine posesorului şi deţinătorilor acestuia.

55. Toţi subiecţii SIA ICCSB, precum şi solicitantul informaţiilor ce conţin date cu caracter personal poartă răspundere conform legislaţiei în vigoare pentru prelucrarea, divulgarea, transmiterea informaţiei din sistem persoanelor terţe, contrar prevederilor legislaţiei în vigoare.

56. Utilizatorii în atribuţiile cărora intră ţinerea SIA ICCSB, introducerea datelor, furnizarea informaţiilor şi asigurarea funcţionării SIA ICCSB poartă răspundere personală în conformitate cu legislaţia în vigoare, pentru completitudinea, autenticitatea, veridicitatea, integritatea informaţiei, precum şi pentru păstrarea şi utilizarea ei.

57. Pentru asigurarea funcţionalităţii eficiente şi neîntrerupte a SIA ICCSB, schimbul informaţional de date SIA ICCSB este asigurat în regim non-stop.

58. Funcţionarea SIA ICCSB se suspendă de către deţinător sau la demersul persoanei responsabile din cadrul Serviciului de asigurarea funcţionalităţii sistemului informaţional şi resurselor informaţionale la nivel local, după coordonarea prealabilă cu posesorul, în caz de apariţie a uneia dintre următoarele situaţii:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software şi hardware al SIA ICCSB;

2) la încălcarea cerinţelor sistemului securităţii informaţiei, dacă aceasta prezintă pericol pentru funcţionarea SIA ICCSB;

3) în cazul apariţiei dificultăţilor tehnice în funcţionarea complexului de mijloace software şi hardware al SIA ICCSB;

4) la cererea scrisă a posesorului.

NOTĂ INFORMATIVĂ

la proiectul Hotărîrii Guvernului privind aprobarea Regulamentului cu privire la organizarea și funcționarea Sistemului Informațional Automatizat de Informare şi Comunicare privind Prevenirea și Combaterea Spălării Banilor

1. Denumirea autorului şi, după caz, a participanţilor la elaborarea proiectului
Serviciul Prevenirea și Combaterea Spălării Banilor
2. Condiţiile ce au impus elaborarea proiectului de act normativ şi finalităţile urmărite
Proiectul hotărîrii Guvernului privind aprobarea Regulamentului cu privire la organizarea și funcționarea Sistemului informațional automatizat de informare și comunicare privind combaterea spălării banilor (SIA ICCSB) a fost elaborat în vederea realizării prevederilor Legii nr. 308 din 22 decembrie 2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și a Hotărîrii Guvernului nr. 14 din 18 ianuarie 2019 cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat de informare și comunicare privind combaterea spălării banilor în vederea implementării unui sistem electronic eficient de raportare și analiză a activităților sau a tranzacțiilor suspecte de spălare a banilor, de infracțiuni asociate acestora și de finanțare a terorismului care cad sub incidența legii sus-menționate. Conceptul a fost elaborat în conformitate cu Legea nr. 982-XVI din 11 mai 2000 cu privire la accesul la informații; Legea nr. 1069-XIV din 22 iunie 2000 cu privire la informatică; Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare și la resursele informaționale de stat; Legea nr. 71-XVI din 22 martie 2007 cu privire la registre; Legea nr. 241-XVI din 15 noiembrie 2007 cu privire la comunicațiile electronice; Legea nr. 133 din 8 iulie 2011 cu privire la protecția datelor cu caracter personal; Hotărîrea Guvernului nr. 735 din 11 iunie 2002 cu privire la sistemele speciale de telecomunicații ale Republicii Moldova; Regulamentul tehnic RT 38370656-022: 2006 „Procesele ciclului de viață al software-ului”, aprobat prin Hotărârea Ministerului Tehnologiei Informației și Comunicațiilor nr. 78 din 1 iunie 2006.
3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislaţiei naţionale cu legislaţia Uniunii Europene
Întru implementarea prevederilor Directivei 2015/849[1] privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, precum şi a standardelor FATF privind recomandările de păstrare a informației și raportarea tranzacțiilor suspecte.
4. Principalele prevederi ale proiectului şi evidenţierea elementelor noi
Regulamentului cu privire la organizarea și funcționarea SIA ICCSB stabilește mecanismul de funcţionare a sistemului informațional automatizat de informare și comunicare al Serviciului Prevenirea și Combaterea Spălării Banilor, cum ar fi destinația și scopul creării sale, funcțiile de bază și circuitele funcționale, documentele principale, obiecte informaționale și datele sistemului, identificatorii entității de informare de bază, scenariile de bază, inclusiv procesele de informare de bază, amenințările la adresa securității informațiilor și cerințele privind securitatea și protecția datelor. Regulamentul reflectă temeiurile şi procedura acordării, suspendării/revocării drepturilor de acces la SIA ICCSB, precum şi regimul juridic de utilizare a datelor din sistem, în scopul evitării riscului de accesare neautorizată a datelor sistemului. SIA ICCSB reprezintă un sistem național de informare și comunicare al Serviciului Prevenirea și Combaterea Spălării Banilor, ce include resurse informaționale de stat care cuprinde datele

[1] Jurnalul Oficial al Uniunii Europene nr. L141/73 din 05 iunie 2015.

sistematizate privind activitățile și tranzacțiile suspecte în ceea ce privește spălarea banilor, infracțiunile ce vizează acest domeniu și finanțarea terorismului, precum și alte informații relevante colectate de Serviciul prevenirea și combaterea spălării banilor în conformitate cu prevederile Legii nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului. SIA ICCSB **are ca scop** colectarea, verificarea și analizarea informațiilor privind relațiile financiare și economice ale persoanelor fizice și juridice care pot fi legate de activitatea de spălare a banilor, infracțiunile asociate acestora și de acțiunile de finanțare a terorismului, activități ce țin de identificarea, stabilirea sursei și urmărirea bunurilor utilizate, obținute din aceste infracțiuni, a fondurilor teroriștilor și a altor bunuri care sînt sau pot fi obiect al măsurilor asiguratorii și/sau al confiscării, precum și activități de investigare a dimensiunii rețelei criminale și a gradului de criminalitate aferente.
5. Fundamentarea economico-financiară
Aprobarea proiectului Hotărîrii Guvernului va contribui la colectarea și procesarea promptă a informațiilor necesare privind relațiile financiare și economice în scopul prevenirii și combaterii spălării banilor și finanțării terorismului; crearea unei resurse analitico-informaționale departamentale a Serviciului Prevenirea și Combaterea Spălării Banilor; organizarea unei colaborări eficiente și a schimbului de informații între Serviciul Prevenirea și Combaterea Spălării Banilor, entitățile raportoare și alte organizații competente la nivel național și internațional; organizarea evidenței analitice și statistice, analiza informațiilor și evaluarea riscurilor de spălare a banilor și de finanțare a terorismului. Implementarea prezentului Regulament nu presupune cheltuieli dat fiind faptul că echipamentul a fost donat de către partenerii externi.
6. Modul de încorporare a actului în cadrul normativ în vigoare
Proiectul se încorporează perfect în sistemul actelor normative și nu va necesita modificarea altor acte legislative sau normative.
7. Avizarea şi consultarea publică a proiectului
Proiectul Hotărîrii Guvernului privind aprobarea Regulamentului cu privire la organizarea și funcționarea „Sistemului informațional automatizat de informare și comunicare privind combaterea spălării banilor” a fost plasat pe pagina web oficială a Serviciului Prevenirea și Combaterea Spălării Banilor și Finanțării Terorismului, la compartimentul *Legislație*, subcompartimentul *Proiecte.*
8. Constatările expertizei anticorupție
9. Constatările expertizei de compatibilitate
10. Constatările expertizei juridice
11. Constatările altor expertize

Director **Vasile ŞARCO**
Serviciul Prevenirea şi
Combaterea Spălării Banilor

Sinteza obiecţiilor şi propunerilor la proiectul Hotărîrii Guvernului cu privire la aprobarea Regulamentului cu privire la organizarea și funcționarea Sistemului informațional automatizat de informare și comunicare privind prevenirea și combaterea spălării banilor

Nr.	Prevederea proiectului	Propunerea de modificare	Autoritatea	Comentarii
1.	**Proiectul Hotărîrii Guvernului** 3. Agenția de Guvernare Electronică, în calitate de operator al platformei guvernamentale tehnologice comune (MCloud), va asigura integrarea SIA ICCSB, garantînd accesul la resursele informaționale de stat, conform normelor de acces reglementate.	**Proiectul Hotărîrii Guvernului** Pct.3 de exclus, deoarece acesta contravine pct.3 și 5 din Hotărârea Guvernului nr.128/2014 „Privind platforma tehnologică guvernamentală comună (MCloud)", care prevede că Instituția publică „Agentia de Guvernare Electronică" (AGE) are calitatea de dezvoltator al platformei MCloud, în timp ce Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică" (STISC) îi revine calitatea de posesor al acestei platforme, iar migrarea sistemelor informaționale noi pe platforma MCloud se realizează în baza acordurilor dintre STISC şi posesorul sistemului respectiv, AGE neavând atribuții în acest sens.	Agenția de Guvernare Electronică	**Se acceptă parțial** La pct.3 al Proiectului Hotărîrii de Guvern va fi indicat Serviciul Tehnologia Informației și Securitate Cibernetică" (STISC) ca posesor al acestei platforme.
2.	Proiectul Regulamentului -	**Proiectul Regulamentului** Considerăm necesar să reiterăm obiecția AGE expusă în cadrul avizării proiectului Concepției tehnice a Sistemului informațional automatizat de informare şi comunicare privind prevenirea şi combaterea spălării banilor (SIA ICCSB) referitoare la obligativitatea găzduirii sistemelor informaționale existente și celor noi pe platforma	Agenția de Guvernare Electronică	**Nu se acceptă** Conform atribuțiilor stipulate la art. 19, alin. (1) lit. m) al Legii 308 din 22.12.2017, Serviciul prevenirea și combaterea spălării banilor „creează și menține un sistem informațional în domeniul său de activitate, inclusiv pagina web oficială, și

		MCloud, reutilizării platformei MCloud și neadmiterii creării de noi infrastructuri proprii centralizate de servere și echipamente de stocare (hardware), inclusiv procurarea licențelor pentru componentele (software) infrastructurilor nou-create. Astfel, cu toate că la aprobarea, prin Hotărârea Guvernului nr.14/2019, a Concepției tehnice a SIA ICCSB, în pct.21 din aceasta, s-a prevăzut că infrastructura sistemului informațional automatizat în cauză să fie realizată prin implementarea unui sistem informatic care va fi găzduit pe platforma tehnologică a Serviciului Prevenirea și Combaterea Spălării Banilor (SPCSB), cu păstrarea copiilor de rezervă pe platforma MCloud, considerăm imperativ ca această neconcordanță cu cadrul normativ aferent utilizării platformei MCloud, admisă la modelarea conceptuală a SIA ICCSB, să fie reparată la promovarea proiectului Regulamentului cu privire la organizarea și funcționarea SIA ICCSB, prezentat spre coordonare. În acest context, accentuăm repetat că un sistem informațional nu poate fi găzduit concomitent atât pe platforma MCloud, cât și pe platforma tehnologică a SPCSB.		asigură funcționarea acestuia, precum și protecția, securitatea și accesul limitat la datele deținute;” Astfel, prin obligativitatea găzduirii SIA ICCSB pe platforma tehnologică guvernamentală comună MCloud, SPCSB va întâmpina dificultăți în asigurarea mentenanței și bunei funcționalități a sistemului. În această ordine de idei, considerăm necesară găzduirea SIA ICCSB pe platforma tehnologică a SPCSB, cu păstrarea copiilor de rezervă pe platforma tehnologică guvernamentală comună MCloud. Totodată, menționăm că sistemul informațional deținut de către SPCSB a fost evaluat în cadrul celei de a 5-a runde de evaluare de către Comitetul Moneyval, în cadrul căreia experții au menționat capacitate deplină a Serviciului de a activa independent și autonom atît din punct de vedere operațional cît și tehnologic. În acest context, orice

		În baza argumentelor expuse, la pct.6, după subpct.6), propunem de completat proiectul Regulamentului cu un subpunct nou, care va deveni subpct.7) și va prevedea o atribuție nouă pentru SPCSB, după cum urmează: **„7) asigură migrarea SIA ICCSB pe platforma tehnologică guvernamentală comună (MCloud), în conformitate cu Hotărârea Guvernului nr.128/2014 „Privind platforma tehnologică guvernamentală comună (MCloud)”;**”. Mai mult, această atribuție a SPCSB se întemeiază și pe calitatea Serviciului de beneficiar al platformei MCloud, conform anexei nr.2 la Hotărârea Guvernului nr.128/2014.		modificarea la componenta IT a Serviciului va avea ca efect *diminuarea/reducerea punctajului/scorului* obținut în cadrul raportului de evaluare și va fi subminat principiul de independență a Serviciului.
3.	Nota informativă	În aceeași ordine de idei, pornind de la faptul că SIA ICCSB urmează a fi găzduit pe platforma MCloud, ceea ce presupune preluarea de către STISC a funcțiilor de administrare tehnică și menținere a sistemelor informaționale respective, considerăm necesar de revizuit **fundamentarea economico-financiară din nota informativă** la proiect, deoarece potrivit SPCSB, la moment, aceste servicii sunt externalizate, iar Serviciul este nevoit să suporte cheltuieli pentru achiziționarea lor.	Agenția de Guvernare Electronică	**Se acceptă parțial** Nu implică cheltuieli de achiziționare, deoarece echipamentul a fost donat de către partenerii externi.

4.	2. *registrator* – angajat al entității raportoare împuternicit cu atribuţii partajate de introducere sau generare a informaţiei în SIA ICCSB; 8. Registratori sînt Entitățile raportoare specificate în art. 4 din Legea 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, prin intermediul angajaţilor acestora împuterniciţi cu atribuţii de acces în sistem, în baza atribuţiilor acordate prin lege, regulamente, specificaţiile din statul de personal al entităților raportoare, profilului de acces al resursei informaţionale.	Constatăm că în textul proiectului Regulamentului apare o neconcordanță în privința termenului de „registrator”. Dacă la pct.2 registratorul este definit ca angajat al entității raportoare, deci persoană fizică, atunci la pct.8 se menționează că registratori sunt entitățile raportoare, care pot fi persoane fizice sau juridice. Astfel, pentru evitarea confuziei dintre noțiunea de „registrator” și cel de „entități raportoare”, propunem definirea clară a acesteia, cu păstrarea sensului în tot textul proiectului.	Agenția de Guvernare Electronică	**Se acceptă**
5.	8. Registratori sînt Entitățile raportoare specificate în art.4 din Legea 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, prin intermediul angajaţilor acestora împuterniciţi cu atribuţii de acces în sistem, în baza atribuţiilor acordate prin lege, regulamente, specificaţiile din statul de personal al entităților raportoare, profilului de acces al resursei informaţionale. 11. Fiecare registrator (persoană juridică) trebuie să prevadă în statul de personal o funcţie responsabilă de introducerea datelor în SIA ICCSB. Numele, prenumele şi datele de contact ale persoanelor angajate în aceste funcţii, precum şi orice modificări cu privire la datele acestora se comunică deținătorului.	În conformitate cu art.4 din Legea nr.308/2007 și pct.2 din Regulamentul prezentat spre avizare, în noțiunea de „entități raportoare” se includ atât persoanele fizice, cât și persoanele juridice. Pe de altă parte, pct.8 din Regulament stipulează că „Registratori sunt Entitățile raportoare specificate în art.4 din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, prin intermediul angajaților acestora împuterniciți cu atribuții de acces în sistem..”, iar la pct.11 este prevăzut că „Fiecare registrator trebuie să prevadă în statul de personal o funcție responsabilă de introducerea datelor în SIA ICCSB”. Astfel, în	Agenția de Guvernare Electronică	**Se acceptă**

		varianta actuală, ar rezulta că fie entitățile raportoare – persoane fizice care nu dispun de angajați sunt excluși din reglementare, fie aceștia vor fi obligați să angajeze personal împuternicit cu atribuții de acces în sistem sau să dispună de stat de personal angajat. Totuși, categoria persoanelor fizice indicate la art.4 din Legea 308/2017 include o categorie largă de persoane fizice, cum ar fi avocați, notari, alți liber-profesioniști, persoanele fizice care practică activități cu metale prețioase și pietre prețioase, etc. În context, se propune a fi reformulat pct. 8 și 11, astfel încât persoanele fizice care se încadrează la definiția entității raportoare să poată avea, după caz, calitatea de registratori nu doar prin intermediul angajaților, ci personal, dacă nu au angajați desemnați în acest scop.		
6.	24. Obiectele informaţionale de bază ale SIA ICCSB sînt: 7) solicitare Grup EGMONT ieşire;	În pct.24 subpct.7) și în alte puncte din Regulament se utilizează noțiunea „EGMONT”, care este un termen specific, ceea ce ar putea cauza dificultăți în interpretare și aplicare. Prin urmare, propunem definirea termenului respectiv la pct.2 din Regulament. Totodată, ținând cont de prevederile Hotărârii Guvernului nr.336/2010 „Privind recunoașterea dobândirii de către Centrul pentru Combaterea Crimelor	Agenția de Guvernare Electronică	**Se acceptă**

		Economice și Corupției a statutului de membru cu drepturi depline al Grupului EGMONT”, am putea concluziona că termenul utilizat ar trebui să fie „Grupului EGMONT”.		
7.	42. SIA ICCSB utilizează următoarele servicii electronice guvernamentale de platformă: 1) serviciul electronic guvernamental de autentificare și control al accesului (MPass), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), aprobat prin Hotărârea Guvernului nr.1090/2013; 2) serviciul electronic guvernamental integrat de semnătură electronică (MSign), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental integrat de semnătură electronică (MSign), aprobat prin Hotărârea Guvernului nr.405/2014; 3) serviciul electronic guvernamental de jurnalizare (MLog), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental de jurnalizare (MLog), aprobat prin Hotărârea Guvernului nr.708/2014.	Pornind de la faptul că pct.42 conține descrieri ale unor servicii electronice guvernamentale de platformă, care sunt definite deja în alte acte normative, pentru evitarea reproducerii normelor complementare, în conformitate cu art.55 alin.(5) din Legea nr.100/2017 cu privire la actele normative, considerăm necesar și suficient să se facă doar trimiteri la elementul structural respectiv din actele în cauză. Astfel, propunem expunerea pct.42 în următoarea redacție: „42. SIA ICCSB utilizează următoarele servicii electronice guvernamentale de platformă: 1) serviciul electronic guvernamental de autentificare și control al accesului (MPass), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), aprobat prin Hotărârea Guvernului nr.1090/2013; 2) serviciul electronic guvernamental integrat de semnătură electronică (MSign), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental integrat de semnătură electronică (MSign),	Agenția de Guvernare Electronică	**Se acceptă**

		aprobat prin Hotărârea Guvernului nr.405/2014; 3) serviciul electronic guvernamental de jurnalizare (MLog), definit în pct.2 din Regulamentul privind serviciul electronic guvernamental de jurnalizare (MLog), aprobat prin Hotărârea Guvernului nr.708/2014.”.		
8.	58. Funcţionarea SIA ICCSB se suspendă de către deţinător sau la demersul persoanei responsabile din cadrul Serviciului de asigurarea funcţionalităţii sistemului informaţional şi resurselor informaţionale la nivel local, după coordonarea prealabilă cu posesorul, în caz de apariţie a uneia dintre următoarele situaţii: 1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software şi hardware al SIA ICCSB; 2) la încălcarea cerinţelor sistemului securităţii informaţiei, dacă aceasta prezintă pericol pentru funcţionarea SIA ICCSB; 3) în cazul apariţiei dificultăţilor tehnice în funcţionarea complexului de mijloace software şi hardware al SIA ICCSB; 4) la cererea scrisă a posesorului.	La pct. 58, subpct. 2) se exclude, deoarece Codul Civil al Republicii Moldova aprobat prin Legea nr.1107/2002 nu prevede ”circumstanțele de forță majoră”	Serviciul Tehnologia Informației și securitate cibernetică	**Se acceptă**
9.	59. În cazul apariţiei circumstanţelor de forţă majoră şi a dificultăţilor tehnice în funcţionarea complexului de mijloace software şi hardware al SIA ICCSB din vina terţelor persoane, este posibilă suspendarea funcţionării SIA ICCSB, cu informarea subiecţilor SIA ICCSB prin mijloacele tehnice disponibile.	La pct. 59 textul ”circumstanțelor de forță majoră și a” se exclude, este valabilă argumentarea expusă pentru pct. 58	Serviciul Tehnologia Informației și securitate cibernetică	**Se acceptă**

SERVICIUL
PREVENIREA ŞI COMBATEREA
SPĂLĂRII BANILOR

MD-2004, mun. Chişinău, bd. Ştefan cel Mare şi Sfânt 198, Tel. (+373) 22-257-243, www.spcsb.gov.md, office@spcsb.gov.md

02/2-11-1733 din 31.12.2019

Cancelaria de Stat

Prin prezenta, Serviciul Prevenirea şi Combaterea Spălării Banilor transmite alăturat cererea pentru înregistrarea proiectului de hotărîre a Guvernului privind aprobarea Regulamentului cu privire la organizarea şi funcţionarea *„Sistemului informaţional automatizat de informare şi comunicare privind combaterea spălării banilor”*.

CERERE

Nr. crt.	**Criterii de înregistrare**	**Nota autorului**
1.	Tipul şi denumirea proiectului	Proiectul de hotărîre a Guvernului privind aprobarea Regulamentului cu privire la organizarea şi funcţionarea *„Sistemului informaţional automatizat de informare şi comunicare privind combaterea spălării banilor”*
2.	Autoritatea care a elaborat proiectul	Serviciul Prevenirea şi Combaterea Spălării Banilor
3.	Justificarea depunerii cererii (indicaţia corespunzătoare sau remarca precum că proiectul este elaborat din iniţiativa autorului)	Proiectul de hotărîre a Guvernului a fost elaborat în vederea realizării prevederilor Legii nr. 308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, precum şi în scopul implementării unui sistem electronic eficient de raportare şi analiză a activităţilor sau a tranzacţiilor suspecte de spălare a banilor, de infracţiuni asociate acestora şi de finanţare a terorismului care cad sub incidenţa legii sus-menţionate.
4.	Lista autorităţilor şi instituţiilor a căror avizare este necesară	1. Ministerul Justiţiei 2. Ministerul Finanţelor (Serviciul Fiscal de Stat)

Digitally signed by Şarco Vasile
Date: 2020.01.02 16:32:16 EET
Reason: MoldSign Signature
Location: Moldova

		3. Ministerul Afacerilor Interne *(Inspectoratul General al Poliției de Frontieră)* 4. Serviciul Vamal 5. Agenția Servicii Publice 6. Agenția de Guvernare Electronică 7. I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică
5.	Termenul-limită pentru depunerea avizelor/expertizelor	5 zile lucrătoare
6.	Numele, prenumele, funcția și datele de contact ale persoanei responsabile de promovarea proiectului	Donciu Alexandru, Șef serviciu cooperare națională și internațională Tel. 022-257-318, E-mail: alexandru.donciu@spcsb.gov.md
7.	Anexe (proiectul actului care se solicită a fi înregistrat, nota informativă cu documentele de însoțire)	1. Proiectul de hotărîre a Guvernului privind aprobarea Regulamentului cu privire la organizarea și funcționarea *„Sistemului informațional automatizat de informare și comunicare privind combaterea spălării banilor”;* 2. Nota informativă la Proiectul de hotărîre a Guvernului; 3. Regulament cu privire la organizarea și funcționarea *„Sistemului informațional automatizat de informare și comunicare privind combaterea spălării banilor”.* 4. Sinteza obiecților și propunerilor
8.	Data și ora depunerii cererii	31.12.2019
9.	Semnătura	

Director **Vasile ȘARCO**