

SINTEZA

obiecțiilor și propunerilor (recomandărilor) la proiectul hotărârii Guvernului privind modificarea Hotărârii Guvernului nr. 834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră (număr unic. 572/MAI/2021)

Participantul la avizare (expertizare)/ consultare publică	Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
Agencia de Guvernare Electronică Aviz nr. 3007-103 din 24.12.2021	I. Obiecțiile Conceptul SIIPF trebuie de completat cu normă care să prevadă că acest sistem informațional este găzduit pe platforma tehnologică guvernamentală comună (MCloud) – infrastructura informațională guvernamentală comună care funcționează în baza tehnologiei de „cloud computing” găzduită în infrastructura consolidată de centre de date. Obligația instituțiilor guvernamentale de a găzdui sistemele informaționale existente pe platforma MCloud sau, după caz, de a le migra pe această platformă tehnologică este stabilită expres în pct.4 și, respectiv, pct.5 din Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud). Mai mult, obligația consolidării în platforma MCloud a centrelor de date din posesia sau deținute de Inspectoratul General al Poliției de Frontieră din subordinea Ministerului Afacerilor Interne se impune și conform pct.7 din Anexa nr.4 la Hotărârea Guvernului nr.414/2018.	<p>Nu se acceptă</p> Conform prevederilor art. 14 din Legea nr. 100/2017 cu privire la actele normative, hotărârea Guvernului este un act care se adoptă de către Guvern întru exercitarea atribuțiilor Guvernului și pentru organizarea executării legilor. Astfel, transmiterea (<i>prin hotărâre a Guvernului</i>) Sistemului informațional integrat al Poliției de Frontieră (<i>SIIPF</i>) din administrarea autorității administrative în administrarea Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică” (<i>STISC</i>), vine în contradicție cu prevederile Legii nr. 283/2011 cu privire la Poliția de Frontieră, întrucât art. 6 alin. (3) lit. c) prevede drept atribuție a Poliției de Frontieră gestiunea și dezvoltarea sistemelor informaționale integrate, precum și stocarea și prelucrarea informațiilor din acestea. Mai mult, Poliția de Frontieră, prin eliberarea din sistemul informațional a datelor despre traversarea frontierei de stat, în conformitate cu lit. e) a aceleiași norme, acordă asistență și servicii cetățenilor. Subsidiar, menționăm prevederile art. 7 alin. (1) lit. h) din Legea prenotată, care stabilește dreptul Poliției de Frontieră să țină evidența persoanelor, a

mijloacelor de transport și a datelor reale necesare pentru asigurarea regimului frontierei de stat, regimului zonei de frontieră și a regimului în punctele de trecere a frontierei de stat și să dețină în acest scop sisteme informaționale.

La fel, art. 10 alin. (1) expune că pentru executarea eficientă a atribuțiilor sale Poliția de Frontieră are dreptul de a colecta, prelucra și păstra informațiile despre persoanele și mijloacele de transport care traversează frontiera de stat, de a crea și utiliza baze de date informaționale proprii, precum și de a utiliza bazele de date ale altor unități, în conformitate cu prevederile legislației cu privire la protecția datelor cu caracter personal.

De asemenea, Legea nr. 71/2007 cu privire la registre (*fiind legea specială aplicabilă asupra tuturor tipurilor de registre, indiferent de forma de proprietate și modul de ținere a acestora*) stabilește la art. 19 alin. (1) că ținerea registrelor se efectuează în strictă conformitate cu regulile de ținere a registrelor stipulate în regulamentul cu privire la modul de ținere a registrului respectiv.

Accentuăm că legea specială menționată prevede expres ce act normativ subordonat legii reprezintă cadrul normativ pentru ținerea registrelor; în cazul particular, acesta fiind Hotărârea Guvernului nr. 834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră.

Așadar, Regulamentul privind modul de ținere a Registrului care formează Sistemul informațional integrat al Poliției de Frontieră, aprobat prin Hotărârea Guvernului nr. 834/2008, stabilește la pct. 7 că Inspectoratul General al Poliției de

Frontieră este posesor, deținător și registrator al SIIPF.

Un alt aspect important, luând în considerație prevederile art. 24 alin. (1) din Legea nr. 71/2007 cu privire la registre (*Răspunderea pentru integritatea datelor registrului o poartă deținătorul acestuia*), în situația în care SIIPF ar fi fost transmis către STISC, de jure deținător al Sistemului, conform cadrului normativ, rămânea în continuare Inspectoratul General al Poliției de Frontieră, acesta fiind responsabil de integritatea datelor registrului, fără a avea posibilitatea de a o asigura, de facto.

Subsecvent, datele introduse și prelucrate în SIIPF ca și consemne, constituie în multe cazuri date și informații atribuite la secret de stat, ce țin de securitatea statului. Apărarea informațiilor în domeniul securității statului este reglementată de art. 16 și art. 17 din Legea nr. 618/1995 securității statului. În calitatea sa de organ al securității statului (*a se vedea art. 13 din Legea nr. 619/1995 privind organele securității statului*) și în conformitate cu prevederile art. 9 din Legea nr. 619/1995 privind organele securității statului, Poliția de Frontieră are dreptul să prelucreze astfel de informații și să creeze sisteme informative în acest scop, iar angajații acesteia poartă răspundere pentru divulgarea informațiilor, potrivit art. 29 din Legea prenotată.

Totodată, potrivit art. 4 alin. (3), lit. c) și d) din Legea nr. 245/2008 cu privire la secretul de stat, sistemul național de protecție a secretului de stat este destinat să garanteze că informațiile atribuite la secret de stat sunt accesibile exclusiv persoanelor

îndreptățite să le cunoască în legătură cu îndeplinirea atribuțiilor de serviciu sau în baza unui alt temei legal și să asigure securitatea sistemelor de telecomunicații, a sistemelor informaționale și a rețelelor de transmitere a secretului de stat.

Astfel, reieșind din faptul că încălcarea regulilor de securitate a sistemului informatic reprezintă o infracțiune, în conformitate cu prevederile art. 261 din Codul penal al Republicii Moldova nr. 985/2002, precum și divulgarea secretului de stat, conform art. 344 din același act normativ, coroborat cu prevederile actelor normative enunțate, conform cărora Inspectoratul General al Poliției de Frontieră este deținător și posesor al sistemului, acesta din urmă (*sau angajații entității*) ar putea fi atras la răspundere penală pentru utilizarea neautorizată a informațiilor, divulgarea acestora sau pentru administrarea necorespunzătoare a centrului de date, în contextul în care centrul de date și bunurile aferente ar fi fost transmise STISC.

Mai mult, intervin și impedimente de ordin organizațional și tehnic, din momentul în care infrastructura sistemului informațional și echipamentele hardware interacționează și sunt localizate în aceeași încăpere cu cele ale sistemului de comunicații speciale TETRA. Camera tehnică centrală TETRA a Inspectoratului General al Poliției de Frontieră (*Main Switch Office (MSO)*), este parte componentă a tuturor locațiilor tehnice din țară în număr de 92 site-uri, pe baza acestei infrastructuri fiind create:

- rețeaua radio securizată în standard TETRA, subsistemul de bază a Rețelei de telecomunicații

		<p>capabilă să asigure comunicarea cifrată între utilizatori. De infrastructura TETRA beneficiază mai multe entități: instituțiile subordonate Ministerului Afacerilor Interne – Inspectoratul General al Poliției de Frontieră, Inspectoratul General al Poliției, Inspectoratul General pentru Situații de Urgență, Serviciul tehnologii informaționale etc., precum și Serviciul Vamal, Ministerul Sănătății, Muncii și Protecției Sociale, Serviciul Național Unic pentru Apelurile de Urgență 112, cu extinderea treptată a utilizatorilor din alte domenii publice;</p> <ul style="list-style-type: none">- supraveghere video;- rețeaua telefonică VoIP;- sistem de transmitere a datelor prin radio-releu;- intranet securizat;- sistemul fix de termoviziune- sistemul de detecție și alertă- sistemul de acces control în subdiviziuni- sistemul depistarea radiației- interpelări și introducerea informației în linie în baze de date departamentale;- integrarea altor servicii, sincronizarea informațiilor din diferite sisteme. <p>Echipamentele de rețea care asigură funcționalitatea rețelei informaționale a Poliției de Frontieră sunt amplasate în camera tehnică centrală TETRA, în caz de nefuncționare, Inspectoratul General al Poliției de Frontieră nu va fi capabil să reacționeze prompt la problemă, din cauza că nu va avea acces la camera tehnică centrală TETRA.</p> <p>Suplimentar riscului de imposibilitate a intervenirii rapide în cazul deficiențelor tehnice, la pierderea</p>
--	--	---

parțială sau totală a comunicațiilor, persistă riscul dereglării întregului proces de coordonare între entitățile utilizatoare a sistemului de radiocomunicații în standard TETRA, la nivel de țară, de asemenea, riscul divulgării informațiilor atribuite la secret de stat, vulnerabilitatea integrității fizice a locațiilor Poliției de Frontieră.

Menționăm că actualmente sistemul TETRA este utilizat pentru schimbul de date on-line în SIIPF (*traversări ale frontierei de stat, consemne la frontieră, neautorizări, planificarea activității patrulilor din subdiviziuni, evidența infracționalității la frontieră etc.*) și, potrivit conceptului, acesta este separat de alte sisteme naționale și nu poate fi amplasat/transmis în alt sistem.

Cât privește răspunderea pentru administrarea sistemelor informaționale și de telecomunicații, mai este de menționat că toate serverele de date și aplicații amplasate în camera tehnică centrală TETRA sunt primite din diverse proiecte de finanțare externă (*în mare parte sunt din proiectul TETRA și fac parte din sistemul TETRA*). Inspectoratul General al Poliției de Frontieră, în calitate sa de beneficiar, are angajamentul față de donatori ca toate sistemele hardware-software să fie utilizate/administrate conform scopului și exclusiv de către beneficiar.

Totodată, se conturează imposibilitatea implementării Acordului dintre Guvernul RM și Cabinetul de Miniștri al Ucrainei cu privire la organizarea schimbului de informație privind persoanele și mijloacele de transport cu care

		<p>persoanele traversează frontiera de stat moldo-ucraineană, aprobat prin Hotărârea Guvernului nr. 84/2016, proiect finanțat de către Organizația Internațională pentru Migrație.</p> <p>Partea software-hardware a acestui proiect, conform art. 3 din Acord, trebuie să fie administrată/implementată doar de Inspectoratul General al Poliției de Frontieră, iar măsurile tehnice și organizatorice sunt clar descrise în art. 7. Riscul este ca partea Donatoare Organizația Internațională pentru Migrație, cât și Partea Ucraineană, să nu accepte derularea în continuare a proiectului în caz că atribuțiile de administrare și mentenanță a sistemului vor fi transmise în întregime unor terți (<i>STISC</i>).</p>
	<p>Luând în considerare faptul că principalul scop al proiectului constă în unificarea, la nivelul Sistemului informațional integrat al Poliției de Frontieră (în continuare – <i>SIIPF</i>), a multiplelor permise, eliberate de către Poliția de Frontieră, stabilirea ținerii evidenței acestor permise exclusiv în format electronic și digitalizarea serviciilor publice aferente, considerăm că se impune completarea Conceptului SIIPF cu norme care să prevadă integrarea acestui sistem informațional cu sisteme informaționale partajate – SI reutilizabile, instituite de Guvern, care asigură funcționalități generice pentru alte sisteme informaționale de stat. Pornind de la destinația și scopul SIIPF, considerăm că pentru dezvoltarea acestuia este necesară integrarea acestuia cu:</p> <p>Platforma de interoperabilitate (MConnect) – în calitate de soluție tehnică destinată asigurării schimbului de date între sistemele informaționale deținute de participanții la schimbul de date, în conformitate cu Legea nr.142/2018 cu privire la schimbul de date și interoperabilitate. Platforma MConnect a fost instituită prin Hotărârea Guvernului nr.211/2019 cu privire la platforma de</p>	<p>Se acceptă Proiectul a fost completat conform obiecției.</p>

interoperabilitate (MConnect), iar obligația integrării de către instituțiile guvernamentale, din contul mijloacelor financiare proprii, a sistemelor informaționale pe care le dețin cu platforma MConnect.

Serviciul electronic guvernamental de autentificare și control al accesului (MPass) – utilizat pentru autentificarea și controlul accesului în cadrul sistemelor informaționale de stat. Din prevederile pct.4 din Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), rezultă obligația instituțiilor guvernamentale cărora acestea le sunt incidente, să integreze cu Serviciul MPass, propriile sisteme informaționale.

Serviciul electronic guvernamental integrat de semnătură electronică (MSign) – utilizat în calitate de mecanism integrator, securizat și flexibil, al diferitelor soluții de aplicare și verificare a autenticității semnăturii electronice de către utilizatori, inclusiv în contextul utilizării sistemelor informaționale și a serviciilor electronice. Conform, pct.4 din Hotărârea Guvernului nr.405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign), instituțiile guvernamentale au obligația de a integra Serviciul MSign în serviciile publice electronice noi și sistemele informaționale aferente, inclusiv cele în curs de dezvoltare.

Serviciul guvernamental de jurnalizare (MLog) – scopul căruia este de a oferi un mecanism securizat și flexibil de jurnalizare și audit, asigurând evidența evenimentelor, în contextul utilizării sistemelor informaționale. Obligația respectivă se conține în pct. 4 din Hotărârea Guvernului nr.708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog), din care rezultă că instituțiile guvernamentale vor integra, din contul mijloacelor financiare proprii, sistemele informaționale noi, inclusiv cele în curs de dezvoltare, cu Serviciul MLog. În acest context, subliniem necesitatea indicării exprese a listei evenimentelor care vor fi jurnalizate în serviciul MLog. Or, trebuie să se rețină că acest

	<p>serviciu nu este destinat log-urilor interne, operaționale (ce țin de funcționarea sistemului), ci este utilizat doar pentru jurnalizarea, log-area unor evenimente cu valoare de business (în sens de business process), evenimentelor care comportă anumite efecte sau consecințe importante (spre exemplu, evenimentele de prelucrare a datelor cu caracter personal, semnarea unui document, luarea unei decizii, etc.).</p> <p>Serviciul guvernamental de notificare electronică (MNotify) – în scopul asigurării notificării utilizatorilor SIIPF, în special a solicitanților de permise sau pentru comunicarea restricțiilor impuse în Zona de Frontieră. Obligația integrării de către instituțiile guvernamentale a serviciilor publice electronice și sistemelor informaționale aferente, inclusiv celor în curs de dezvoltare, cu serviciul MNotify, este stabilită în pct.4 din Hotărârea Guvernului nr.376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify).</p>	
	<p>II. Propunerile (recomandările)</p>	
	<p>Pe tot parcursul proiectului cuvintele „permisul de aflare în zona de frontieră”, la orice formă gramaticală, de substituit cu cuvintele „permisul de acces în zona de frontieră”, la forma gramaticală corespunzătoare, în vederea uniformizării cu prevederile art.30 din Legea nr.215/2011 cu privire la frontiera de stat a Republicii Moldova.</p>	<p>Nu se acceptă Prin proiect se urmărește unificarea evidenței mai multor tipuri de permise statuate de prevederile Hotărârii Guvernului nr. 297/2017 pentru implementarea Legii nr. 215/2011 cu privire la frontiera de stat a Republicii Moldova (<i>permisul de activitate în punctele de trecere a frontierei de stat, permisul de acces în zona de frontieră, permisul pentru ambarcațiune</i>).</p>
	<p><i>La pct.1 subpct.1) (modificări la Conceptul tehnic al Sistemul informațional integrat al Poliției de Frontieră (în continuare - SIIPF):</i> În contextul obiecțiilor de ordin general expuse supra, lit.a) urmează a fi completată cu trimiterile la alte acte normative relevante, care</p>	<p>Se acceptă parțial Proiectul a fost completat conform propunerii, cu excepția referinței la Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud), având în vedere</p>

	<p>reglementează utilizarea platformei MCloud și a sistemelor informaționale partajate nominalizate: Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud). Legea nr. 142/2018 privind schimbul de date și interoperabilitate; Hotărârea Guvernului nr.211/2019 cu privire la platforma de interoperabilitate (MConnect); Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass); Hotărârea Guvernului nr.405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign); Hotărârea Guvernului nr.708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog); Hotărârea Guvernului nr.376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify).</p>	argumentarea de la compartimentul obiecții.
	<p><i>La pct.1 subpct.1) (modificări la Conceptul tehnic al Sistemul informațional integrat al Poliției de Frontieră (în continuare - SIIPF):</i> După lit.e), considerăm necesar de completat proiectul cu prevederi noi care să prevadă completarea pct.18 din Concept cu norme vizând efectuarea schimbului de date între SIIPF cu alte sisteme informaționale prin intermediul platformei de interoperabilitate (MConnect), în scopul conformării cadrului normativ în domeniului schimbului de date și interoperabilității. În acest context, propunem de completat proiectul cu următoarea normă: „... la punctul 18 alineatul unu va avea următorul cuprins: „Pentru asigurarea formării corecte a resursei informaționale a SIIPF, acesta va interacționa, prin intermediul platformei de interoperabilitate (MConnect), cu următoarele sisteme informaționale de stat:”</p>	<p>Se acceptă Proiectul a fost completat conform propunerii.</p>
	<p><i>La pct.1 subpct.1) (modificări la Conceptul tehnic al Sistemul</i></p>	<p>Nu se acceptă</p>

	<p><i>informațional integrat al Poliției de Frontieră (în continuare - SIIPF):</i> După lit.e), considerăm necesar de completat proiectul cu prevederi noi care să prevadă găzduirea SIIPF pe platforma MCloud. În context, propunem de completat Conceptul SIIPF cu pct.19¹ cu următorul cuprins: „19¹. SIIPF este găzduit pe platforma tehnologică guvernamentală comună (MCloud), care permite accesul, la cerere, pe bază de rețea la totalitatea configurabilă a resurselor de calcul virtualizabile (de exemplu rețele, servere, echipamente de stocare, aplicații și servicii), ce pot fi puse rapid la dispoziție cu un efort minim de administrare sau interacțiune cu furnizorul acestor servicii. În acest fel, SIIPF va putea fi ușor extins pe verticală, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.”.</p>	<p>A se vedea argumentarea de la compartimentul obiecții.</p>
	<p><i>La pct.1 subpct.1) (modificări la Conceptul tehnic al Sistemul informațional integrat al Poliției de Frontieră (în continuare - SIIPF):</i> După lit.e), considerăm necesar de completat proiectul cu prevederi noi care să prevadă integrarea cu și reutilizarea de către SIIPF a funcționalităților sistemelor informaționale partajate. Astfel, propunem de completat Conceptul SIIPF cu pct.201 cu următorul cuprins: „20¹. Integrarea cu sisteme informaționale partajate Pentru asigurarea funcționării și dezvoltării SIIPF este integrat cu și reutilizează funcționalitățile generice ale sistemelor informaționale partajate, în special, dar nu exclusiv: 1) <i>serviciul electronic guvernamental de autentificare și control al accesului (MPass)</i> – pentru autentificarea și controlul accesului în cadrul sistemului, utilizând mecanismul de autentificare prin semnătură electronică; 2) <i>serviciul electronic guvernamental integrat de semnătură</i></p>	<p>Se acceptă Proiectul a fost completat conform propunerii.</p>

	<p><i>electronică (MSign) – pentru semnarea documentelor electronice;</i></p> <p>3) <i>platforma de interoperabilitate (MConnect) – pentru organizarea schimbului de date și interoperabilității cu alte sisteme informaționale de stat;</i></p> <p>4) <i>serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiunilor (evenimentelor) produse în cadrul sistemului;</i></p> <p>5) <i>serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea registratorilor și utilizatorilor.</i></p>	
Agencia de Guvernare Electronica Aviz nr. 3007-41 din 29.03.2022	I. Obiectiile	
	Lipsa de obiectii	-
	II. Propunerile (recomandarile)	
	<p>Lit.a) de completat cu lit.r), care să conțină trimitere la Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud).</p> <p>După lit.f), de completat cu o literă nouă, care să prevadă completarea Conceptului cu o normă privind găzduirea SIIPF pe platforma MCloud, cu următorul cuprins:</p> <p><i>„19^l. SIIPF este găzduit pe platforma tehnologică guvernamentală comună (MCloud), care permite accesul, la cerere, pe bază de rețea, la totalitatea configurabilă a resurselor de calcul virtualizabile (de exemplu rețele, servere, echipamente de stocare, aplicații și servicii), ce pot fi puse rapid la dispoziție cu un efort minim de administrare sau interacțiune cu furnizorul acestor servicii. În acest fel, SIIPF va putea fi ușor extins pe verticală, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.”.</i></p> <p>În susținerea obiectiilor respective, reiterăm că obligativitatea găzduirii pe platforma MCloud a sistemelor informaționale de stat din posesia Inspectoratului General al Poliției de Frontieră din subordinea Ministerului Afacerilor Interne corespunde întocmai politicii de stat în domeniul eTransformării guvernării, orientate spre</p>	<p>Nu se acceptă</p> <p>Proiectul este elaborat în scopul realizării Planului de acțiuni al Guvernului pentru anii 2021-2022 (<i>acțiunea nr. 24.9.1.</i>), precum și în scopul asigurării realizării politicii de stat în domeniul managementului integrat al frontierei de stat, prin digitalizarea serviciilor și simplificarea obținerii permisului de acces în zona de frontieră, iar aceste propuneri sunt suplimentare și nu se referă la proiect, deviind totodată de la scopul proiectului. De menționat că, în conformitate cu prevederile Legii nr. 100/2017 cu privire la actele normative și Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, avizul se întocmește la proiect (<i>în cazul nostru de modificare a unui act normativ</i>), dar nu la actul normativ supus modificării.</p> <p>Totodată, la 15.11.2021 pe pagina web oficială a Ministerului Afacerilor Interne și pe platforma de participare (<i>particip.gov.md</i>) a fost publicat anunțul referitor la inițierea elaborării proiectului, nefiind</p>

	<p>economisirea bugetului TI în sectorul public prin reducerea costului plătit pentru achiziționarea echipamentului hardware și a licențelor software, precum și consolidarea și optimizarea centrelor de date în sectorul public, și se întemeiază pe dispozițiile pct.4 subpct.1) din Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud).</p> <p>Mai mult, obligația consolidării în platforma MCloud a centrelor de date din posesia sau deținute de IGPF se impune și pornind de la faptul că acesta este inclus, la pct.7, în Lista entităților posesoare/deținătoare de centre de date supuse consolidării în platforma tehnologică guvernamentală comună (MCloud) în mod <i>prioritar</i> - Anexa nr.4 la Hotărârea Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.</p> <p>În această ordine de idei, considerăm că argumentele invocate de autor de neacceptare a obiecțiilor enunțate, care se bazează pe principiul ierarhiei actelor normative, sunt nepotrivite, deoarece nu există nici o contradicție sau divergență între actele normative respective și dispozițiile art.6 alin.(3) lit.c) și e) și art.7 alin.(1) lit.h) din vine în contradicție cu prevederile Legii nr. 283/2011 cu privire la Poliția de Frontieră. Astfel, faptul găzduirii SIIPF, sub aspect tehnologic, pe platforma MCloud nu va aduce nici o atingere sau va periclita exercitarea de către IGPF a funcțiilor și realizarea responsabilităților ce-i revin în tripla sa calitate de posesor, deținător și registrator al SIIPF, în temeiul articolelor indicate din Legea nr.283/2011 cu privire la Poliția de Frontieră, coroborate cu reglementările-cadru din Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat și din Legea nr.71/2007 cu privire la registre, precum și în conformitate cu prevederile Hotărârii Guvernului nr.834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră.</p> <p>De asemenea, considerăm că nu pot fi reținute nici argumentele</p>	<p>înaintate care va propune de modificare a Hotărârii Guvernului nr. 834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră.</p> <p>Subsidiar, conform prevederilor art. 14 din Legea nr. 100/2017 cu privire la actele normative, hotărârea Guvernului este un act care se adoptă de către Guvern întru exercitarea atribuțiilor Guvernului și pentru organizarea executării legilor.</p> <p>Astfel, transmiterea (<i>prin hotărâre a Guvernului</i>) Sistemului informațional integrat al Poliției de Frontieră (<i>SIIPF</i>) din administrarea autorității administrative în administrarea Instituției Publice „Serviciul Tehnologie Informației și Securitate Cibernetică” (<i>STISC</i>), vine în contradicție cu prevederile Legii nr. 283/2011 cu privire la Poliția de Frontieră, întrucât art. 6 alin. (3) lit. c) prevede drept atribuție a Poliției de Frontieră gestiunea și dezvoltarea sistemelor informaționale integrate, precum și stocarea și prelucrarea informațiilor din acestea. Mai mult, Poliția de Frontieră, prin eliberarea din sistemul informațional a datelor despre traversarea frontierei de stat, în conformitate cu lit. e) a aceleiași norme, acordă asistență și servicii cetățenilor.</p> <p>Subsidiar, menționăm prevederile art. 7 alin. (1) lit. h) din Legea prenotată, care stabilește dreptul Poliției de Frontieră să țină evidența persoanelor, a mijloacelor de transport și a datelor reale necesare pentru asigurarea regimului frontierei de stat, regimului zonei de frontieră și a regimului în punctele de trecere a frontierei de stat și să dețină în acest scop sisteme informaționale.</p> <p>La fel, art. 10 alin. (1) expune că pentru executarea</p>
--	---	--

	<p>autorului privind sensibilitatea datelor prelucrate în SIIPF. În acest context, este oportun să menționăm că în Lista entităților publice, autorităților administrative autonome față de Guvern, beneficiare ale platformei MCloud (Anexa nr.2 la Hotărârea Guvernului nr.128/2014), sunt incluse, spre exemplu, și alte organe de ocrotire a normelor de drept - Centrul Național Anticorupție, Procuratura Generală, Curtea Supremă de Justiție, care, de asemenea, administrează date cu accesibilitate limitată. În altă ordine de idei, este necesar de precizat că funcțiile și drepturile Instituției publice „Serviciul Tehnologia Informației și Securitatea Cibernetică”, ca și posesor și deținător al platformei MCloud, sunt stabilite expres în Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud). Astfel, STISC îi revine funcția de alocare și disponibilizare a resurselor din platforma MCloud, iar beneficiarilor serviciilor din platforma MCloud le revin funcțiile de asigurare a integrității sistemelor informaționale proprii găzduite pe platforma, protejării datelor procesate în cadrul acestor SI, precum și crearea și stocarea copiilor de rezervă.</p>	<p>eficientă a atribuțiilor sale Poliția de Frontieră are dreptul de a colecta, prelucra și păstra informațiile despre persoanele și mijloacele de transport care traversează frontiera de stat, de a crea și utiliza baze de date informaționale proprii, precum și de a utiliza bazele de date ale altor unități, în conformitate cu prevederile legislației cu privire la protecția datelor cu caracter personal.</p> <p>De asemenea, Legea nr. 71/2007 cu privire la registre (<i>fiind legea specială aplicabilă asupra tuturor tipurilor de registre, indiferent de forma de proprietate și modul de ținere a acestora</i>) stabilește la art. 19 alin. (1) că ținerea registrelor se efectuează în strictă conformitate cu regulile de ținere a registrelor stipulate în regulamentul cu privire la modul de ținere a registrului respectiv.</p> <p>Accentuăm că legea specială menționată prevede expres ce act normativ subordonat legii reprezintă cadrul normativ pentru ținerea registrelor; în cazul particular, acesta fiind Hotărârea Guvernului nr. 834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră.</p> <p>Așadar, Regulamentul privind modul de ținere a Registrului care formează Sistemul informațional integrat al Poliției de Frontieră, aprobat prin Hotărârea Guvernului nr. 834/2008, stabilește la pct. 7 că Inspectoratul General al Poliției de Frontieră este posesor, deținător și registrator al SIIPF.</p> <p>Un alt aspect important, luând în considerație prevederile art. 24 alin. (1) din Legea nr. 71/2007 cu privire la registre (<i>Răspunderea pentru integritatea datelor registrului o poartă deținătorul</i></p>
--	--	--

acestui), în situația în care SIIPF ar fi fost transmis către STISC, de jure deținător al Sistemului, conform cadrului normativ, rămânea în continuare Inspectoratul General al Poliției de Frontieră, acesta fiind responsabil de integritatea datelor registrului, fără a avea posibilitatea de a o asigura, de facto.

Subsecvent, datele introduse și prelucrate în SIIPF ca și consemne, constituie în multe cazuri date și informații atribuite la secret de stat, ce țin de securitatea statului. Apărarea informațiilor în domeniul securității statului este reglementată de art. 16 și art. 17 din Legea nr. 618/1995 securității statului. În calitatea sa de organ al securității statului (*a se vedea art. 13 din Legea nr. 619/1995 privind organele securității statului*) și în conformitate cu prevederile art. 9 din Legea nr. 619/1995 privind organele securității statului, Poliția de Frontieră are dreptul să prelucreze astfel de informații și să creeze sisteme informative în acest scop, iar angajații acesteia poartă răspundere pentru divulgarea informațiilor, potrivit art. 29 din Legea prenotată.

Totodată, potrivit art. 4 alin. (3), lit. c) și d) din Legea nr. 245/2008 cu privire la secretul de stat, sistemul național de protecție a secretului de stat este destinat să garanteze că informațiile atribuite la secret de stat sunt accesibile exclusiv persoanelor îndreptățite să le cunoască în legătură cu îndeplinirea atribuțiilor de serviciu sau în baza unui alt temei legal și să asigure securitatea sistemelor de telecomunicații, a sistemelor informaționale și a rețelelor de transmitere a secretului de stat.

Astfel, reieșind din faptul că încălcarea regulilor de

		<p>securitate a sistemului informatic reprezintă o infracțiune, în conformitate cu prevederile art. 261 din Codul penal al Republicii Moldova nr. 985/2002, precum și divulgarea secretului de stat, conform art. 344 din același act normativ, coroborat cu prevederile actelor normative enunțate, conform cărora Inspectoratul General al Poliției de Frontieră este deținător și posesor al sistemului, acesta din urmă (<i>sau angajații entității</i>) ar putea fi atras la răspundere penală pentru utilizarea neautorizată a informațiilor, divulgarea acestora sau pentru administrarea necorespunzătoare a centrului de date, în contextul în care centrul de date și bunurile aferente ar fi fost transmise STISC.</p> <p>Mai mult, intervin și impedimente de ordin organizațional și tehnic, din momentul în care infrastructura sistemului informațional și echipamentele hardware interacționează și sunt localizate în aceeași încăpere cu cele ale sistemului de comunicații speciale TETRA. Camera tehnică centrală TETRA a Inspectoratului General al Poliției de Frontieră (<i>Main Switch Office (MSO)</i>), este parte componentă a tuturor locațiilor tehnice din țară în număr de 92 site-uri, pe baza acestei infrastructuri fiind create:</p> <ul style="list-style-type: none">- rețeaua radio securizată în standard TETRA, subsistemul de bază a Rețelei de telecomunicații capabilă să asigure comunicarea cifrată între utilizatori. De infrastructura TETRA beneficiază mai multe entități: instituțiile subordonate Ministerului Afacerilor Interne – Inspectoratul General al Poliției de Frontieră, Inspectoratul General al Poliției, Inspectoratul General pentru
--	--	--

		<p>Situații de Urgență, Serviciul tehnologii informaționale etc., precum și Serviciul Vamal, Ministerul Sănătății, Muncii și Protecției Sociale, Serviciul Național Unic pentru Apelurile de Urgență 112, cu extinderea treptată a utilizatorilor din alte domenii publice;</p> <ul style="list-style-type: none">- supraveghere video;- rețeaua telefonică VoIP;- sistem de transmitere a datelor prin radio-releu;- intranet securizat;- sistemul fix de termoviziune- sistemul de detecție și alertă- sistemul de acces control în subdiviziuni- sistemul depistarea radiației- interpelări și introducerea informației în linie în baze de date departamentale;- integrarea altor servicii, sincronizarea informațiilor din diferite sisteme. <p>Echipamentele de rețea care asigură funcționalitatea rețelei informaționale a Poliției de Frontieră sunt amplasate în camera tehnică centrală TETRA, în caz de nefuncționare, Inspectoratul General al Poliției de Frontieră nu va fi capabil să reacționeze prompt la problemă, din cauza că nu va avea acces la camera tehnică centrală TETRA.</p> <p>Suplimentar riscului de imposibilitate a intervenirii rapide în cazul deficiențelor tehnice, la pierderea parțială sau totală a comunicațiilor, persistă riscul dereglării întregului proces de coordonare între entitățile utilizatoare a sistemului de radiocomunicații în standard TETRA, la nivel de țară, de asemenea, riscul divulgării informațiilor atribuite la secret de stat, vulnerabilitatea integrității</p>
--	--	--

fizice a locațiilor Poliției de Frontieră.

Menționăm că actualmente sistemul TETRA este utilizat pentru schimbul de date on-line în SIIPF (*traversări ale frontierei de stat, consemne la frontieră, neautorizări, planificarea activității patrulilor din subdiviziuni, evidența infracționalității la frontieră etc.*) și, potrivit conceptului, acesta este separat de alte sisteme naționale și nu poate fi amplasat/transmis în alt sistem.

Cât privește răspunderea pentru administrarea sistemelor informaționale și de telecomunicații, mai este de menționat că toate serverele de date și aplicații amplasate în camera tehnică centrală TETRA sunt primite din diverse proiecte de finanțare externă (*în mare parte sunt din proiectul TETRA și fac parte din sistemul TETRA*). Inspectoratul General al Poliției de Frontieră, în calitate sa de beneficiar, are angajamentul față de donatori ca toate sistemele hardware-software să fie utilizate/administrate conform scopului și exclusiv de către beneficiar.

Totodată, se conturează imposibilitatea implementării Acordului dintre Guvernul RM și Cabinetul de Miniștri al Ucrainei cu privire la organizarea schimbului de informație privind persoanele și mijloacele de transport cu care persoanele traversează frontiera de stat moldo-ucraineană, aprobat prin Hotărârea Guvernului nr. 84/2016, proiect finanțat de către Organizația Internațională pentru Migrație.

Partea software-hardware a acestui proiect, conform art. 3 din Acord, trebuie să fie

		<p>administrată/implementată doar de Inspectoratul General al Poliției de Frontieră, iar măsurile tehnice și organizatorice sunt clar descrise în art. 7. Riscul este ca partea Donatoare Organizația Internațională pentru Migrație, cât și Partea Ucraineană, să nu accepte derularea în continuare a proiectului în caz că atribuțiile de administrare și mentenanță a sistemului vor fi transmise în întregime unor terți (STISC).</p>
	<p>Propunem de perfecționat sub aspect redacțional modificarea de la lit.f) și de o expune în următoarea redacție: <i>„În scopul formării corecte a resursei informaționale a SIIPF și asigurării furnizării datelor din această resursă autorităților/instituțiilor publice, în limitele competențelor stabilite de actele normative, SIIPF va interacționa, prin intermediul platformei de interoperabilitate (MConnect), cu următoarele sisteme informaționale de stat:”.</i></p>	<p>Se acceptă Proiectul a fost modificat conform propunerii.</p>
	<p>Totodată, în calitate de autoritate competentă de asigurarea schimbului de date și a interoperabilității, AGE a analizat suplimentar redacția în vigoare a Regulamentului privind modul de ținere a Registrului care formează Sistemul informațional integrat al Poliției de Frontieră. Astfel, în scopul conformării dispozițiilor art.29 alin.(1) lit.a) și alin.(2) din Legea nr.71/2007 cu privire la registre, care prevăd că punerea la dispoziție a datelor din registru se realizează prin acordarea accesului sancționat prin platforma de interoperabilitate în conformitate, care se efectuează în conformitate cu legislația în vigoare cu privire la schimbul de date și interoperabilitate, pentru asigurarea respectării principiilor fundamentale ale schimbului de date și interoperabilității, statuate în art.4 lit.a) - c) din Legea nr.142/2018 cu privire la schimbul de date și interoperabilitate, precum și conformării dispozițiilor art.6 alin.(3) din aceeași Lege, care stabilesc pentru participanții publici, inclusiv IGPF, obligația „să efectueze schimbul de date prin intermediul</p>	<p>Nu se acceptă Proiectul este elaborat în scopul realizării Planului de acțiuni al Guvernului pentru anii 2021-2022 (acțiunea nr. 24.9.1.), precum și în scopul asigurării realizării politicii de stat în domeniul managementului integrat al frontierei de stat, prin digitalizarea serviciilor și simplificarea obținerii permisului de acces în zona de frontieră, iar aceste propuneri sunt suplimentare și nu se referă la proiect, deviind totodată de la scopul proiectului. De menționat că, în conformitate cu prevederile Legii nr. 100/2017 cu privire la actele normative și Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, avizul se întocmește la proiect (în cazul nostru de modificare a unui act normativ), dar nu la actul normativ supus</p>

	<p>platformei de interoperabilitate și să asigure condițiile tehnice necesare realizării schimbului de date”, cadrului normativ în domeniul schimbului de date și interoperabilitate, considerăm necesar completarea pct.1 subpct.2), cu amendamentul la Capitolul V din Regulament, în partea ce ține de regimul juridic de utilizare a datelor din SIIPF, după cum urmează:</p> <p>„g) <i>punctul 37 va avea următorul cuprins:</i></p> <p><i>37. Punerea la dispoziție a datelor din SIIPF și furnizarea lor de către deținătorul SIIPF autorităților și instituțiilor publice se realizează prin intermediul platformei de interoperabilitate (MConnect) în conformitate cu prevederile cadrului normativ în domeniul schimbului de date și interoperabilității, în condițiile în care acestea invocă un scop și un temei legal pentru prelucrarea setului de date solicitat și respectă cerințele de securitate și confidențialitate ce decurg din regimul juridic al datelor vizate.”.</i></p>	<p>modificării.</p> <p>Totodată, la 15.11.2021 pe pagina web oficială a Ministerului Afacerilor Interne și pe platforma de participare (<i>particip.gov.md</i>) a fost publicat anunțul referitor la inițierea elaborării proiectului, nefiind înaintate careva propuneri de modificare a Hotărârii Guvernului nr. 834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră.</p>
Serviciul Tehnologia Informației și Securitate Cibernetică Aviz nr. 1.4/1651/44-21 din 15.12.2021	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	Lipsa de propuneri	-
Serviciul Tehnologia Informației și Securitate Cibernetică Aviz nr. 1.4/567/22 din 28.03.2022	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	Lipsa de propuneri	-
Ministerul Finanțelor Aviz nr. 07/4-04/531/1335 din 20.12.2021	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	Lipsa de propuneri	-
Ministerul	I. Obiecțiile	

Finanțelor Aviz nr. 07/4-04/154 din 31.03.2022	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	Lipsa de propuneri	-
Ministerul Economiei Aviz nr. 07-17 din 04.01.2022	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	În scopul delimitării clare a competențelor între instituțiile responsabile de ținerea evidenței străinilor, precum și reieșind din faptul că funcția de evidență a străinilor la prima trecere a frontierei de stat în legătură cu intrarea în Republica Moldova ține de domeniul de competență al Poliției de Frontieră, considerăm oportun excluderea din Registrul de Stat al Populației a conturului automatizat de evidență și control al trecerii frontierei de stat al Republicii Moldova ("CONTROL-D"), și includerea acestui contur automatizat în Sistemul informațional integrat al Poliției de Frontieră. Astfel, toată informația privind traversarea frontierei de stat de către străini urmând a fi stocată în cadrul unui singur sistem – Sistemul informațional integrat al Poliției de Frontieră.	Nu se acceptă Subiectul abordat este obiectul de reglementare al unui alt proiect de hotărâre de Guvern care vizează multiaspectual modificarea Hotărârii Guvernului nr. 333/2002 (<i>a se vedea proiectul cu numărul unic 155/MEI/ASP/2021</i>).
Ministerul Economiei Aviz nr. 07-953 din 04.04.2022	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	În contextul promovării modificărilor în Hotărârea Guvernului nr. 834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră, vă informăm că proiectul cu număr unic 155/MEI/ASP/2021, ce prevedea modificarea Hotărârii Guvernului nr.333/2002 pentru aprobarea Concepției sistemului informațional automatizat „Registrul de stat al populației” și Regulamentului cu privire la Registrul de stat al populației” a fost remis în adresa dlui Iurie Țurcanu, Vicepremier pentru digitalizare, prin scrisoarea ME nr.07-4827 din 02.11.2021, în scopul luării deciziei privind promovarea acestuia conform competenței, însă nu a fost promovat până în prezent. În acest sens, ar fi oportun de examinat posibilitățile de armonizare	Nu se acceptă Proiectul este elaborat în scopul realizării Planului de acțiuni al Guvernului pentru anii 2021-2022 (<i>acțiunea nr. 24.9.1.</i>), precum și în scopul asigurării realizării politicii de stat în domeniul managementului integrat al frontierei de stat, prin digitalizarea serviciilor și simplificarea obținerii permisului de acces în zona de frontieră, iar această propunere este una suplimentară și nu se referă la proiect, deviind totodată de la scopul proiectului. De menționat că, în conformitate cu prevederile Legii nr. 100/2017 cu privire la actele normative și

	<p>a prevederilor proiectului prezentat la avizare cu proiectul 155/MEI/ASP/2021, în contextul în care MAI nu a prezentat aviz la ultimul.</p> <p>Astfel, rămâne actuală problema delimitării clare a competențelor între instituțiile responsabile de ținerea evidenței străinilor, prin modificarea simultană a Hotărârii Guvernului nr. 834/2008 și Hotărârii Guvernului nr.333/2002, în sensul excluderii din Registrul de Stat al Populației a conturului automatizat de evidență și control al trecerii frontierei de stat al Republicii Moldova ("CONTROL-D"), și includerii acestui contur automatizat în Sistemul informațional integrat al Poliției de Frontieră, toată informația privind traversarea frontierei de stat de către străini urmând a fi stocată în cadrul unui singur sistem – Sistemul informațional integrat al Poliției de Frontieră.</p>	<p>Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, avizul se întocmește la proiect (<i>în cazul nostru de modificare a unui act normativ</i>), dar nu la actul normativ supus modificării.</p> <p>Totodată, la 15.11.2021 pe pagina web oficială a Ministerului Afacerilor Interne și pe platforma de participare (<i>particip.gov.md</i>) a fost publicat anunțul referitor la inițierea elaborării proiectului, nefiind înaintate careva propuneri de modificare a Hotărârii Guvernului nr. 834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră.</p>
Serviciul de Informații și Securitate Aviz nr. 18/1429 din 16.12.2021	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
Serviciul de Informații și Securitate Aviz nr. 18/458 din 30.03.2022	Lipsa de propuneri	-
	I. Obiecțiile	
	Lipsa de obiecții	-
Centrul Național pentru Protecția Datelor cu Caracter Personal Aviz nr. 04-01/3608 din 28.12.2021	II. Propunerile (recomandările)	
	Lipsa de propuneri	-
	Lipsa de obiecții	-
Centrul Național pentru Protecția Datelor cu Caracter	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	

Personal Aviz nr. 04-01/829 din 31.03.2022	Lipsa de propuneri	-
Ministerul Justiției Expertiza juridică nr. 04/10297 din 20.12.2021	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	În conformitate cu art. 52 alin. (2) din <i>Legea nr. 100/2017 cu privire la actele normative</i> , punctele de regulă, nu au denumire sunt expuse fără utilizarea cuvântului „punct” și se însemnează consecutiv cu numere ordinare, exprimate prin cifre arabe, urmate de punct. Prin urmare, la referința la punctul 5 se va exclude paranteza rotundă (obiecție valabilă și în alte cazuri similare).	Se acceptă Proiectul a fost modificat conform propunerii
	La cuprinsul care se propune la punctul 14 lit. f) din Anexa nr. 1, din sintagma „legislația în vigoare” cuvintele „în vigoare” se vor exclude ca fiind inutile. Regula generală este că referințele la actele normative reprezintă referințe la legislația în vigoare și doar pentru excepțiile de la regulă se va specifica dacă este vorba despre legislația aplicabilă la un anumit moment (obiecție valabilă și la pct. 18 sbp. 6) lit.a) și lit. c)). Totodată, la expresia „antecedentelor penale nestinse” remarcăm că, art. 110 și 111 din <i>Codul penal</i> , prevede, că antecedentele penale reprezintă o stare juridică a persoanei, ce apare din momentul rămîinerii definitive a sentinței de condamnare, generînd consecințe de drept nefavorabile pentru condamnat pînă la momentul stingerii antecedentelor penale sau reabilitării. Astfel, stingerea antecedentelor penale anulează toate incapacitățile și decăderile din drepturi legate de acestea, iar persoanele se consideră ca neavînd antecedente penale	Se acceptă Proiectul a fost modificat conform propunerii
La cuprinsul care se propune la pct. 18 sbp. 6) lit. c) din Anexa nr. 2, cuvintele „de trecere” sunt indicate în mod repetat. Prin urmare, cuvintele indicate în mod repetat se vor exclude.	Se acceptă Proiectul a fost modificat conform propunerii	
Potrivit notei informative, urmare a aprobării proiectului va fi necesară modificarea <i>Hotărîrii Guvernului nr. 297/2017 pentru implementarea Legii nr. 215/2011 cu privire la frontiera de stat a</i>	Nu se acceptă Considerăm judicios ca amendamentele la Hotărârea Guvernului nr. 297/2017 pentru	

	<i>Republicii Moldova.</i> În acest sens, considerăm oportun ca amendamentele la actul normativ enunțat să fie inserate în cadrul unuia și aceluiași proiect.	implementarea Legii nr. 215/2011 cu privire la frontiera de stat a Republicii Moldova să fie operate ulterior executării acțiunii nr. 24.6.9. din Planul de acțiuni al Guvernului pentru anii 2021-2022, aprobat prin Hotărârea Guvernului nr. 235/2021. Astfel, se va asigura un cadru normativ comprehensiv în conformitate cu prevederile Legii nr. 100/2017 cu privire la actele normative.
Ministerul Justiției Expertiza juridică nr. 04/3130 din 04.04.2022	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	La pct. 1 sbp. 1) lit. a), cuvintele „vor avea următoarele cuprinsuri” se vor substitui cu cuvintele „vor avea următorul cuprins”. Totodată, se va ține cont că, potrivit regulilor tehnicii legislative, pentru a evita enumerarea a mai mult de trei elemente de structură consecutive, se utilizează cratima.	Se acceptă Proiectul a fost modificat conform propunerii
	În conformitate cu art. 52 alin. (3) din <i>Legea nr. 100/2017 cu privire la actele normative</i> , subpunctele sunt însemnate cu numere ordinare, exprimate prin cifre arabe, urmate de o paranteză, și se evidențiază printr-o ușoară retragere spre dreapta de la alinierea textului pe verticală. Prin urmare, subpunctele de la pct. 20 ¹ urmează a fi numerotate în forma enunțată.	Se acceptă Proiectul a fost modificat conform propunerii
Centrul Național Anticorupție Expertiza anticorupție nr. EHG22/7826 din 23.03.2022	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	Lipsa de propuneri	-
Centrul Național Anticorupție Aviz nr. 06/2-1856 din 29.03.2022	I. Obiecțiile	
	Lipsa de obiecții	-
	II. Propunerile (recomandările)	
	Lipsa de propuneri	-

Secretar general al ministerului

Serghei DIACONU