

Tabelul comparativ
la proiectul de lege pentru modificarea unor acte normative
(revizuirea cadrului normativ conex Registrului de stat al armelor)

Nr./0	Conținutul normei în vigoare	Modificarea propusă	Conținutul normei după modificare
Conceptul Sistemului informațional automatizat „Registrul de stat al armelor”, aprobat prin Hotărârea Guvernului nr.609/2018			
1.	16. Posesor și deținător al SIA „RSA” este Ministerul Afacerilor Interne - autoritatea care exercită autorizarea, evidența, controlul și supravegherea privind deținerea, portul și folosirea armelor și a munițiilor, precum și operațiunile cu acestea, fiind unica autoritate competentă care reprezintă Republica Moldova în cadrul transferurilor și notificărilor privind armele și munițiile.	1.1.punctul 16 va avea următorul cuprins: „16. Posesorul SIA „RSA” este Ministerul Afacerilor Interne, care asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, funcționarea, mentenanța și dezvoltarea SIA „RSA”.”	16. Posesorul SIA „RSA” este Ministerul Afacerilor Interne, care asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, funcționarea, mentenanța și dezvoltarea SIA „RSA”.
2.	-	1.2. se completează cu punctul 16 ¹ cu următorul cuprins: „16 ¹ . Deținătorul SIA „RSA” este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, responsabil de crearea, administrarea, mentenanța și dezvoltarea sistemului informațional, precum și de exercitarea atribuțiilor de administrator tehnic al acestuia, prin asigurarea nemijlocită a administrării tehnice, mentenanței, dezvoltării SIA „RSA” și implementării cerințelor de securitate stabilite de actele normative în domeniu.”	16 ¹ . Deținătorul SIA „RSA” este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne, responsabil de crearea, administrarea, mentenanța și dezvoltarea sistemului informațional, precum și de exercitarea atribuțiilor de administrator tehnic al acestuia, prin asigurarea nemijlocită a administrării tehnice, mentenanței, dezvoltării SIA „RSA” și implementării cerințelor de securitate stabilite de actele normative în domeniu.
3.	17 ¹ . Administratorul tehnic al SIA „RSA” este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care își exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.	1.3. punctul 17 ¹ se abrogă;	-
4.	53. Scenariul pentru evenimentul informațional „Examinarea tehnică periodică” Prezentarea unui armurier licențiat a armei, a permisului, actului de identitate și dovezii de achitare a tarifului pentru examinarea tehnică. Verificarea țevii, funcționării mecanismelor armei, închizătorului, marcajului, dimensiunilor armei, după caz, încercarea prin tragere.	1.4. la punctul 53, textul „Verificarea se efectuează conform standardelor SM GOST R 50529:2010, SM GOST R 50741:2005, SM GOST R 51612:2001.” se exclude.	53. Scenariul pentru evenimentul informațional „Examinarea tehnică periodică” Prezentarea unui armurier licențiat a armei, a permisului, actului de identitate și dovezii de achitare a tarifului pentru examinarea tehnică. Verificarea țevii, funcționării mecanismelor armei, închizătorului, marcajului,

	Verificarea se efectuează conform standardelor SM GOST R 50529:2010, SM GOST R 50741:2005, SM GOST R 51612:2001. Eliberarea certificatului de corespundere potrivit standardelor, conform modelului din anexa nr.25 la Regulament, valabil pentru o perioadă de 5 ani sau după caz. Procesul-verbal de constatare a neconformităților, conform anexei nr.26 la Regulament. Punerea la evidența primară a documentelor eliberate.		dimensiunilor armei, după caz, încercarea prin tragere. Eliberarea certificatului de corespundere potrivit standardelor, conform modelului din anexa nr.25 la Regulament, valabil pentru o perioadă de 5 ani sau după caz. Procesul-verbal de constatare a neconformităților, conform anexei nr.26 la Regulament. Punerea la evidența primară a documentelor eliberate.
Regulamentul privind modul de ținere a Registrului de stat al armelor, format de Sistemul informațional automatizat „Registrul de stat al armelor”, aprobat prin Hotărârea Guvernului nr.416/2021			
5.		2.1. pe tot cuprinsul textului Regulamentului, sintagma „administratorul tehnic” și cuvintele „administratorul tehnic al”, la orice formă gramaticală, se substituie cu cuvântul „deținătorul”, la forma gramaticală corespunzătoare	
6.	12. Subiecții raporturilor juridice în domeniul creării și funcționării SIA RSA și a SIA e-RSA sunt: 4) administratorul tehnic;	2.2. la punctul 12, subpunctul 4) se abrogă	
7.	15. Inspectoratul General al Poliției din subordinea Ministerului Afacerilor Interne este deținătorul Registrului și asigură, prin intermediul structurilor sale de specialitate de nivel central și local, înregistrarea, actualizarea, sistematizarea și analiza informațiilor din acesta, inclusiv inițierea modificării proceselor de lucru și a cerințelor față de sistemul informațional care asigură formarea acestuia, execută testarea funcțională a sistemului informațional și, după caz, propune scoaterea din exploatare a sistemului informațional sau a unor module ale acestuia.	2.3. punctul 15 va avea următorul cuprins: „15. Deținătorul Registrului este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne.”	15. Deținătorul Registrului este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne.
8.	16. Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică este administratorul tehnic al Registrului și asigură administrarea tehnică a acestuia, inclusiv funcționalitatea lui.	2.4. punctul 16 se abrogă;	-
9.	22. Deținătorul Registrului are următoarele obligații: 12) în cazul incidentelor de securitate, deficiențelor și defecțiunilor apărute în	2.5 la punctul 22: 2.5.1. subpunctul 12) va avea următorul cuprins: „12) remedierea deficiențelor și	22. Deținătorul Registrului are următoarele obligații: 12) remedierea deficiențelor și defecțiunilor apărute în funcționarea Registrului;

	funcționarea Registrului, deținătorul acestuia notifică administratorul tehnic al Registrului pentru întreprinderea măsurilor în vederea depistării sursei de producere a incidentelor și remedierii acestora; 14) gestionarea și păstrarea înregistrărilor de audit intern și extern ale securității operațiilor de prelucrare a datelor cu caracter personal în cadrul SIA RSA și SIA e-RSA, efectuate în privința activității administratorului tehnic al Registrului;	defecțiunilor apărute în funcționarea Registrului;”; 2.5.2. subpunctul 14), textul „ , efectuate în privința activității administratorului tehnic al Registrului” se exclude; 2.5.3. se completează cu subpunctele 16)-24) cu următorul cuprins: „16) întreprinderea măsurilor de prevenire a incidentelor de securitate; 17) prevenirea accesului neautorizat la datele/informațiile/documentele din Registru; 18) asigurarea funcționării Registrului; 19) executarea modificărilor/rectificărilor solicitate în cererile privind erorile de sistem ale SIA RSA și ale SIA e-RSA, erorile cauzate de factorul uman în SIA RSA și SIA e-RSA, incidentele de infrastructură care afectează funcționarea normală a SIA RSA și a SIA e-RSA; 20) asigurarea mentenanței SIA RSA și a SIA e-RSA; 21) asigurarea dezvoltării SIA RSA și a SIA e-RSA, elaborarea și coordonarea cu posesorul Registrului a planului de continuitate al acestor sisteme informaționale; 22) asigurarea implementării cerințelor de securitate stabilite de actele normative în domeniu, inclusiv: a) asigurarea funcționalității și securității logice și cibernetice a SIA RSA și a SIA e-RSA în conformitate cu actele normative în acest domeniu; b) instituirea activităților de control menite să diminueze riscurile privind integritatea datelor din Registru; 23) asigurarea generării periodice a copiilor de rezervă a bazei de date a Registrului; 24) întreprinderea măsurilor necesare pentru depistarea sursei generatoare în cazul incidentului de securitate, efectuarea analizei acestuia și înlăturarea cauzelor și condițiilor care l-au favorizat, cu informarea Centrului	14) gestionarea și păstrarea înregistrărilor de audit intern și extern ale securității operațiilor de prelucrare a datelor cu caracter personal în cadrul SIA RSA și SIA e-RSA,; 16) întreprinderea măsurilor de prevenire a incidentelor de securitate; 17) prevenirea accesului neautorizat la datele/informațiile/documentele din Registru; 18) asigurarea funcționării Registrului; 19) executarea modificărilor/rectificărilor solicitate în cererile privind erorile de sistem ale SIA RSA și ale SIA e-RSA, erorile cauzate de factorul uman în SIA RSA și SIA e-RSA, incidentele de infrastructură care afectează funcționarea normală a SIA RSA și a SIA e-RSA; 20) asigurarea mentenanței SIA RSA și a SIA e-RSA; 21) asigurarea dezvoltării SIA RSA și a SIA e-RSA, elaborarea și coordonarea cu posesorul Registrului a planului de continuitate al acestor sisteme informaționale; 22) asigurarea implementării cerințelor de securitate stabilite de actele normative în domeniu, inclusiv: a) asigurarea funcționalității și securității logice și cibernetice a SIA RSA și a SIA e-RSA în conformitate cu actele normative în acest domeniu; b) instituirea activităților de control menite să diminueze riscurile privind integritatea datelor din Registru; 23) asigurarea generării periodice a copiilor de rezervă a bazei de date a Registrului; 24) întreprinderea măsurilor necesare pentru depistarea sursei generatoare în cazul incidentului de securitate, efectuarea analizei acestuia și înlăturarea cauzelor și condițiilor care l-au favorizat, cu informarea Centrului Național pentru Protecția Datelor cu Caracter Personal.
--	---	---	--

		Național pentru Protecția Datelor cu Caracter Personal.”.	
10.	23. Administratorul tehnic al Registrului are următoarele obligații: 1) remedierea deficiențelor și defecțiunilor apărute în funcționarea Registrului; 2) întreprinderea măsurilor de prevenire a incidentelor de securitate; 3) prevenirea accesului neautorizat la datele/informațiile/documentele din Registru; 4) asigurarea funcționării Registrului; 5) executarea modificărilor/rectificărilor solicitate în cererile privind erorile de sistem ale SIA RSA și ale SIA e-RSA, erorile cauzate de factorul uman în SIA RSA și SIA e-RSA, incidentele de infrastructură care afectează funcționarea normală a SIA RSA și a SIA e-RSA; 6) asigurarea mentenanței SIA RSA și a SIA e-RSA; 7) asigurarea dezvoltării SIA RSA și a SIA e-RSA, elaborarea și coordonarea cu posesorul Registrului a planului de continuitate al acestor sisteme informaționale; 8) asigurarea implementării cerințelor de securitate stabilite de actele normative în domeniu, inclusiv: a) asigurarea funcționalității și securității logice și cibernetice a SIA RSA și a SIA e-RSA în conformitate cu actele normative în acest domeniu; b) instituirea activităților de control menite să diminueze riscurile privind integritatea datelor din Registru; 9) asigurarea generării periodice a copiilor de rezervă a bazei de date a Registrului; 10) întreprinderea măsurilor necesare pentru depistarea sursei generatoare în cazul incidentului de securitate, efectuarea analizei acestuia și înlăturarea cauzelor și condițiilor care l-au favorizat, cu informarea Centrului Național pentru Protecția Datelor cu Caracter Personal.	2.6. punctul 23 se abrogă;	-
11.	29. Deținătorul Registrului are următoarele drepturi:	2.7. punctul 29: 2.7.1. subpunctul 1) va avea următorul cuprins: „1) coordonarea prealabilă a	29. Deținătorul Registrului are următoarele drepturi:

	1) coordonarea prealabilă a proiectului de decizie privind autorizarea, modificarea, suspendarea și revocarea dreptului de acces la Registru al registratorilor, furnizorilor și destinatarilor acestuia, cu înaintarea unei solicitări în acest sens administratorului tehnic al Registrului, prin intermediul structurii de specialitate din subordinea posesorului Registrului abilitată cu atribuții în domeniul protecției datelor cu caracter personal; 2) solicitarea de la subiecții raporturilor juridice ai Registrului de a respecta cerințele de securitate privind accesul la resursa informațională și regulile de exploatare a sistemului informațional în procesul de introducere, vizualizare, completare, modificare, procesare, extragere, invalidare și arhivare a datelor/informațiilor/documentelor în Registru; 3) gestionarea și utilizarea datelor/informațiilor/documentelor din cadrul resurselor introduse în SIA RSA; 4) solicitarea de la registratori și furnizori a informațiilor suplimentare despre obiectele suspuse înregistrării în SIA RSA; 5) înaintarea propunerilor de ordin normativ, tehnic și organizatoric în vederea îmbunătățirii funcționării Registrului.	proiectului de decizie privind autorizarea, modificarea, suspendarea și revocarea dreptului de acces la Registru al utilizatorilor, registratorilor, furnizorilor și destinatarilor acestuia, cu structura de specialitate din cadrul aparatului central al Ministerului Afacerilor Interne, abilitată cu atribuții în domeniul protecției datelor cu caracter personal;”; 2.7.2. se completează cu subpunctele 6)-8) cu următorul cuprins: „6) accesarea și vizualizarea datelor/informațiilor/documentelor din SIA RSA și SIA e-RSA; 7) efectuarea modificărilor de ordin tehnic și organizatoric în vederea îmbunătățirii funcționării Registrului; 8) solicitarea de la registratori și furnizori, la detectarea erorilor și omisiunilor, de a actualiza și corecta datele/informațiile/documentele introduse în Registru.”	1) coordonarea prealabilă a proiectului de decizie privind autorizarea, modificarea, suspendarea și revocarea dreptului de acces la Registru al utilizatorilor, registratorilor, furnizorilor și destinatarilor acestuia, cu structura de specialitate din cadrul aparatului central al Ministerului Afacerilor Interne, abilitată cu atribuții în domeniul protecției datelor cu caracter personal; 2) solicitarea de la subiecții raporturilor juridice ai Registrului de a respecta cerințele de securitate privind accesul la resursa informațională și regulile de exploatare a sistemului informațional în procesul de introducere, vizualizare, completare, modificare, procesare, extragere, invalidare și arhivare a datelor/informațiilor/documentelor în Registru; 3) gestionarea și utilizarea datelor/informațiilor/documentelor din cadrul resurselor introduse în SIA RSA; 4) solicitarea de la registratori și furnizori a informațiilor suplimentare despre obiectele suspuse înregistrării în SIA RSA; 5) înaintarea propunerilor de ordin normativ, tehnic și organizatoric în vederea îmbunătățirii funcționării Registrului. 6) accesarea și vizualizarea datelor/informațiilor/documentelor din SIA RSA și SIA e-RSA; 7) efectuarea modificărilor de ordin tehnic și organizatoric în vederea îmbunătățirii funcționării Registrului; 8) solicitarea de la registratori și furnizori, la detectarea erorilor și omisiunilor, de a actualiza și corecta datele/informațiile/documentele introduse în Registru.”
12.	30. Administratorul tehnic al Registrului are următoarele drepturi:	2.8. punctul 30 se abrogă;	-

	1) accesarea și vizualizarea datelor/informațiilor/documentelor din SIA RSA și SIA e-RSA; 2) efectuarea modificărilor de ordin tehnic și organizatoric în vederea îmbunătățirii funcționării Registrului; 3) solicitarea de la registratori și furnizori, la detectarea erorilor și omisiunilor, de a actualiza și corecta datele/informațiile/documentele introduse în Registru.		
13.	73. Acces la SIA RSA și SIA e-RSA pe plan intern au doar următorii subiecți: 5) Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică. Aceasta are acces doar la conturile funcționale prevăzute la punctul 69, cu drept de vizualizare, modificare, extragere, invalidare și arhivare a datelor/informațiilor din SIA RSA și SIA e-RSA în partea ce ține de evidența: a) respectării regulilor de securitate și a procedurilor în procesul tehnic de introducere, vizualizare, completare, modificare, procesare, extragere, invalidare și arhivare a datelor/informațiilor/documentelor din SIA RSA și SIA e-RSA de către utilizatorii sistemului informațional și resurselor informaționale; b) asigurării administrării tehnice a SIA RSA și a SIA e-RSA, inclusiv a funcționalității acestora; c) asigurării mentenanței SIA RSA și a SIA e-RSA;	2.9. punctul 73 subpunctul 5), textul „Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică” se substituie cu textul „Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne”.	73. Acces la SIA RSA și SIA e-RSA pe plan intern au doar următorii subiecți: 5) Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne. Aceasta are acces doar la conturile funcționale prevăzute la punctul 69, cu drept de vizualizare, modificare, extragere, invalidare și arhivare a datelor/informațiilor din SIA RSA și SIA e-RSA în partea ce ține de evidența: a) respectării regulilor de securitate și a procedurilor în procesul tehnic de introducere, vizualizare, completare, modificare, procesare, extragere, invalidare și arhivare a datelor/informațiilor/documentelor din SIA RSA și SIA e-RSA de către utilizatorii sistemului informațional și resurselor informaționale; b) asigurării administrării tehnice a SIA RSA și a SIA e-RSA, inclusiv a funcționalității acestora; c) asigurării mentenanței SIA RSA și a SIA e-RSA;