

**CENTRUL NAȚIONAL
ANTICORUPȚIE
AL REPUBLICII MOLDOVA**



**НАЦИОНАЛЬНЫЙ ЦЕНТР
ПО БОРЬБЕ С КОРРУПЦИЕЙ
РЕСПУБЛИКИ МОЛDOVA**

MD-2004, mun. Chișinău, bd. Ștefan cel Mare și Sfânt, 198
Tel. 24-36-41

Nr. 06/2-5003 din 21.08 2017
La nr.38-04-6016 din 02.08.2017

Cancelaria de Stat

Prin prezenta, Vă remitem atașat raportul de expertiză anticorupție asupra proiectului de lege cu privire la schimbul de date și interoperabilitate.

Anexă: Raportul de expertiză anticorupție – 8 file.

Director adjunct

Vadim COJOCARU



RAPORT DE EXPERTIZĂ ANTICORUPȚIE

Nr.ELO17/4395 din 25.08.2017

la proiectul de lege cu privire la schimbul de date și interoperabilitate

Prezentul raport de expertiză anticorupție a fost întocmit de Centrul Național Anticorupție al Republicii Moldova în baza Legii nr.780/2001 privind actele legislative, a Legii nr.1104/2002 cu privire la Centrul Național Anticorupție și a Metodologiei de efectuare a expertizei anticorupție, aprobată prin Ordinul nr.179 din 17 noiembrie 2016 a directorului Centrului Național Anticorupție.

I. Analiza riscurilor de corupere a procesului de promovare a proiectului

I.1. Pertinența autorului, categoriei propuse a actului și a procedurii de promovare a proiectului

Autor al proiectului de lege este Guvernul Republicii Moldova, autor nemijlocit – Cancelaria de Stat, ceea ce corespunde art.73 din Constituție.

Categoria actului legislativ propus este lege organică, ceea ce corespunde art.72 din Constituție și art.6-11 din Legea nr.780/2001 privind actele legislative.

I.2. Respectarea rigorilor de transparență în procesul decizional la promovarea proiectului

Conform art.8 al Legii nr.239/2008 privind transparența în procesul decizional „*etapele asigurării transparenței procesului de elaborare a deciziilor sunt:*

- a) informarea publicului referitor la inițierea elaborării deciziei;*
- b) punerea la dispoziția părților interesate a proiectului de decizie și a materialelor aferente acestuia;*
- c) consultarea cetățenilor, asociațiilor constituite în corespundere cu legea, altor părți interesate;*
- d) examinarea recomandărilor cetățenilor, asociațiilor constituite în corespundere cu legea, altor părți interesate în procesul de elaborare a proiectelor de decizii;*
- e) informarea publicului referitor la deciziile adoptate.”*

Potrivit art.12 alin.(2) al legii, „*Termenul de prezentare a recomandărilor asupra proiectelor de decizii va constitui cel puțin 10 zile lucrătoare de la data mediatizării anunțului referitor la inițierea elaborării deciziei sau de la data mediatizării anunțului privind organizarea consultărilor publice.”* Mai mult ca atât, art.11 alin.(2/2) al aceleiași legi prevede că „*Anunțul privind organizarea consultărilor publice și materialele aferente sunt făcute publice cu cel puțin 15 zile lucrătoare înainte de definitivarea*

proiectului de decizie.”

Proiectul supus expertizei a fost plasat pe portalul oficial www.particip.gov.md, fiind asigurat accesul părților interesate la proiectul prenotat, inclusiv cu asigurarea termenului de 10 zile lucrătoare pentru recepționarea propunerilor și/sau obiecțiilor.

Suplimentar, autorul proiectului nu a asigurat informarea publicului referitor la inițierea elaborării prezentului proiect de decizie, condiție prevăzută de art.8 lit.a) din Legea nr.239/2008 privind transparența în procesul decizional.

În consecință, în procesul de promovare a proiectului asigurarea transparenței decizionale stabilite de Legea nr.239/2008 privind transparența în procesul decizional a fost în mare parte asigurată.

I.3. Scopul anunțat și scopul real al proiectului

Potrivit notei informative: *„Scopul principal al proiectului constă în implementarea cadrului de interoperabilitate guvernamental a sistemelor informaționale de stat, prin instituirea bazei juridico-normative pentru utilizarea platformei de interoperabilitate, care ar reglementa procesul de schimb de date prin interconectarea și interoperabilitatea conținutului/resurselor informaționale și procedura de acordare a accesului la registrele și bazele de date de importanță națională pentru toate entitățile din sectorul public, în conformitate cu competențele lor legale și în scopurile conforme legii.”*

Potrivit proiectului: *„Prezenta lege are scopul să faciliteze schimbul de date și interoperabilitatea, atât în scopuri comerciale, cât și necomerciale.”*

Astfel se atestă o neconcordanță între scopul declarat în nota informativă și prevederile proiectului. Or, instituirea unei platforme de interoperabilitate și obligarea prin lege a tuturor consumatorilor și furnizorilor de date să accedă la platforma respectivă cu posibilitatea instituirii unor taxe pentru acest fapt constituie un abuz din partea legiuitorilor și manifestă dubii asupra scopului „nobil” al proiectului. Astfel că, acordarea posibilității de impunere a taxelor pentru furnizarea informației se atestă ca încercarea monopolizării sectorului informațional în servirea scopului financiar a anumitor persoane sau grupuri de interese.

Prin urmare, se constată că scopul declarat de către autor în nota informativă nu corespunde scopului real al proiectului.

I.4. Interesul public și interesele private promovate prin proiect

Proiectul promovează interesele statului de a beneficia de modernizarea sectorului public prin implementarea eficientă a prevederilor legii cu privire la schimbul de date și interoperabilitate, ceea ce este conform interesului public.

Totodată, instituirea unei platforme în care se vor concentra toate datele și informațiile pe țară precum și stabilirea unui scop comercial, poate servi anumitor interese private sau grupuri de interese ceea ce se califică a fi în detrimentul interesului public.

I.5. Justificarea soluțiilor proiectului

I.5.1. Suficiența argumentării din nota informativă. În conformitate cu art.20 al Legii nr.780/2001 privind actele legislative, proiectele de acte legislative sunt însoțite de nota informativă care include:

- a) condițiile ce au impus elaborarea proiectului, inclusiv necesitatea armonizării actului legislativ cu reglementările legislației comunitare, finalitățile urmărite prin implementarea noilor reglementări;
- b) principalele prevederi, locul actului în sistemul legislației, evidențierea elementelor noi, efectul social, economic și de altă natură al realizării lui;
- c) referințele la reglementările corespondente ale legislației comunitare și nivelul compatibilității proiectului de act legislativ cu reglementările în cauză.”

Potrivit autorului, „[...] Platforma de interoperabilitate, a fost instituită conform prevederilor pct. 1 din Hotărârea Guvernului nr.404 din 02.06.2014 „Cu privire la pilotarea platformei de interoperabilitate”, în calitate de soluție tehnică ce asigură schimbul de date dintre sistemele informaționale deținute de ministere, alte autorități administrative centrale subordonate Guvernului și structurile organizaționale din sfera lor de competență (autoritățile administrative din subordine, instituțiile publice și întreprinderile de stat în care ministerul sau altă autoritate administrativă centrală are calitatea de fondator), precum și de instituțiile publice autonome. Platforma respectivă este proprietatea statului, ca parte componentă a platformei tehnologice guvernamentale comune (MCloud). Potrivit pct. 2 subpct 2)-3) din actul normativ menționat, posesor al platformei de interoperabilitate este Cancelaria de Stat, deținător al acesteia - Centrul de Guvernare Electronică (E-Government), iar întreprinderea de Stat „Centrul de telecomunicații speciale” are calitatea de operator tehnico-tehnologic al platformei de interoperabilitate.”

Autorul menționează că: „Inițiativa este o consecință logică a procesului de pilotare a platformei de interoperabilitate, care a fost lansată în luna iunie.2014 și la care au participat Î.S. „CRIS Registru”, Î.S. „Cadastru”, Inspectoratul Fiscal Principal de Stat, Casa Națională de Asigurări Sociale etc. Astfel, în rezultatul pilotării s-a constatat că, sub aspect tehnic, platforma de interoperabilitate este una deplin funcțională. Această permite, la moment, conectarea la platformă în regim de producție a principalelor surse de date din sectorul public, deținute de participanții la pilotare, și realizarea unui schimb de date eficient în cadrul proiectelor de integrare deja realizate. De asemenea, tehnologic platforma de interoperabilitate permite lansarea și a unor proiecte noi de integrare cu platformă a altor sisteme informaționale pentru consumul și/sau furnizarea datelor de către alte entități din sectorul public, ceea ce ar contribui la creșterea calității serviciilor publice prestate persoanelor fizice și juridice și eficientizarea și optimizarea activității acestora.”

Deși autorul aduce numeroase argumente, proiectul nu elucidează necesitatea instituirii unei „Autorități competente” care va dubla atribuțiile și competențele atribuite deja altor entități publice. De asemenea nu este argumentată necesitatea concentrării tuturor informațiilor într-o singură sursă de accesare (platforma de interoperabilitate) în condițiile în care acest fapt va vulnerabiliza securitatea datelor și informațiilor cu accesibilitate limitată.

În consecință, argumentele din nota informativă nu sunt întemeiate iar proiectul nu întrunește exigențele stabilite de prevederile art.20 al Legii nr.780/2001 privind actele legislative.

I.5.2. Argumentarea economico-financiară. Conform art.20 lit.d) al Legii nr.780/2001 privind actele legislative, nota informativă trebuie să conțină „d) fundamentarea economico-financiară în cazul în care realizarea noilor reglementări necesită cheltuieli financiare și de altă natură”.

Potrivit notei informative: „Cheltuielile de implementare a proiectului de lege cu privire la schimbul de date și interoperabilitate se rezumă la costurile de achiziționare, administrare și suportul tehnic al

platformei de interoperabilitate.

Costul total al investiției pentru achiziționarea platformei de interoperabilitate a constituit circa 17,2 mln. lei pe parcursul perioadei anilor 2011-2016, care a fost acoperită din mijloacele Proiectului „e-Transformare a Guvernării”, finanțat de Banca Mondială. Totodată, pe parcursul anilor 2014-2016, valoarea cumulativă a cheltuielilor operaționale legate de administrarea platformei de interoperabilitate (cost de personal și cost de distribuție: instruiți și traininguri) a constituit circa 3,96 mln. lei.

Pentru anii 2017-2019 sunt preconizate cheltuieli de ordin operațional de circa 8,1 mln. lei care includ costuri de personal - circa 4,5 mln. lei, costuri de mentenanță corectivă (suport tehnic acordat de furnizor și găzduirea platformei de interoperabilitate de către Î. S. „Centrul de telecomunicații speciale”) - circa 3,4 mln. lei și cheltuieli de distribuție (instruire și promovare) - circa 209 mii lei, care urmează a fi acoperite din contul bugetului de stat pentru anul respectiv, în ceea ce privește anul curent, în Legea bugetului de stat pentru anul 2017 nr.279 din 16 decembrie 2016, au fost prevăzute mijloace financiare necesare pentru suportul tehnic a platformei în sumă de 2,048 mln. lei, precum și pentru finanțarea consultanților tehnici implicați în efectuarea lucrărilor de integrare a surselor de date administrative cu platforma de interoperabilitate, în contextul modernizării serviciilor publice, în sumă de 2,096 mln. 960 lei.

Aceste cheltuieli sunt justificate de beneficiile pe care le oferă implementarea în continuare a platformei de interoperabilitate pentru facilitarea schimbului de date în sectorul public dintre autoritățile și instituțiile publice pentru creșterea eficienței guvernamentale interne la general și a calității serviciilor publice în special.

Astfel, beneficiul economic al acestei platforme este cuantificat în termeni de micșorare a sarcinii administrative în proces de prestare a serviciilor publice. Pentru determinarea sarcinii administrative la prestarea unui serviciu public, a fost evaluat serviciul “e - Indemnizații”, prestat de Casa Națională de Asigurări Sociale, la nașterea unui copil. Calculul sarcinii administrative a fost efectuat în conformitate cu prevederile Ghidului metodologic privind reingineria serviciilor publice, elaborat în anul 2014 în contextul suportului acordat Cancelariei de Stat în implementarea reformei serviciilor publice.

Potrivit rezultatelor obținute eficiența doar a unui singur serviciu prestat pe baza platformei de interoperabilitate poate atinge o valoare de 1,29 unități, sau cu 29% să micșoreze sarcina administrativă, aferenta proceselor: deplasării către oficiul prestatorului și pregătirii și depunerii setului de documente la oficiul prestatorului (ii), pentru obținerea indemnizației. Ca rezultat, pe parcursul anilor 2017-2019 vor fi obținute cumulativ economii în valoare de 8,2 mln. lei.

Mai mult, raportând la PIB timpul pierdut per tranzacție al beneficiarului de indemnizație, pentru anul 2015 obținem o pierdere estimativă a valorii contribuției “eșuate” în PIB - de 69,1 mln. lei, iar pentru anul 2016 - 33,2 mln. lei.”

II. Analiza generală a factorilor de risc ale proiectului

II.1. Limbajul proiectului

Potrivit art.19 al Legii nr.780/2001 privind actele legislative “textul proiectului de act legislativ se elaborează [...] cu respectarea următoarelor reguli: [...]

c) se utilizează termeni adecvați [...] și de o largă circulație; [...]

e) terminologia utilizată în actul elaborat este constantă și uniformă ca și în celelalte acte legislative și în reglementările legislației comunitare; se va utiliza unul și același termen dacă este corect, iar folosirea lui repetată exclude confuzia; [...]

g) se evită folosirea [...] cuvintelor și expresiilor [...] neutilizabile și/sau cu sens ambiguu;

h) se evită tautologiile juridice; [...]

Textul proiectului este ambiguu și poate fi interpretat. Sunt utilizate formulări neclare și noțiuni care

nu sunt reglementate sau nu sunt caracteristice domeniului de referință cum ar fi: „jurnalizarea datelor”. Aspectele date sunt descrise detaliat în compartimentul III al prezentului Raport de expertiză anticorupție.

II.2. Coerența legislativă a proiectului

În prevederile proiectului au fost identificate norme contradictorii atât între prevederile din proiect cât și prevederile acestuia și Legea nr.780/2011 cu privire la actele legislative și Legea nr.133/2011 privind protecția datelor cu caracter personal. Aspectele date sunt descrise detaliat în compartimentul III al prezentului Raport de expertiză anticorupție.

II.3. Activitatea agenților publici și a entităților publice reglementată în proiect

Proiectul conține reglementări ce se referă la activitatea Guvernului Republicii Moldova în partea ce ține de realizarea programului „e - Transformare a Guvernării” pe sectorul schimbului de date prin intermediul unei platforme de interoperabilitate. În sensul dat, Guvernul va institui „Autoritatea competentă” care va gestiona toate activitățile din domeniul de referință.

În acest sens, prevederile proiectului conțin carențe care ar putea facilita abuzuri și discreții la aplicare. Prin proiect se urmărește instituirea unei autorități suplimentare cu funcții de control, al cărei mecanism de lucru nu este reglementat, la fel și consecințele ce se vor răsfrânge asupra deținătorilor de date ca urmare a presupuselor încălcări stabilite în rezultatele controalelor efectuate de aceasta, eventualele sancțiuni și penalități, etc.

Aspectele date sunt descrise detaliat în compartimentul III al prezentului Raport de expertiză anticorupție.

II.4. Atingeri ale drepturilor omului care pot fi cauzate la aplicarea proiectului

În forma propusă, prevederile proiectului pot aduce atingere dreptului la informație prevăzut de art.34 din Constituția Republicii Moldova, adoptată la 29.07.1994.

III. Analiza detaliată a factorilor de risc și a riscurilor de corupție ale proiectului

1. Art.1 alin.(4) , Art.5 lit.a), b) și c) și art.7 alin.(6)

Art.1 alin.(4) Prezenta lege are scopul să faciliteze schimbul de date și interoperabilitatea, atât în scopuri comerciale, cât și necomerciale.

Art.5 Schimbul de date și interoperabilitatea, se bazează pe următoarele principii:

a) gratuitatea datelor - toate datele deținute de participanții publici, sînt puse la dispoziție altor participanți publici, în mod gratuit. Punerea la dispoziție a datelor deținute de participanții publici către participanți privați, poate fi făcută contra plată

b) disponibilitatea datelor - toate datele deținute de participanții la schimbul de date sunt disponibile în egală măsură pentru orice alt participant la schimbul de date, în baza mandatului legal al acestuia, iar în acest scop sunt asigurate cerințele de interoperabilitate tehnică,

semantică și organizatorică. Participanții la schimbul de date sunt obligați să asigure disponibilitatea tuturor seturilor de date deținute;

c) autenticitatea datelor - toate datele din sistemele informaționale ale participanților la schimbul de date, furnizate prin intermediul platformei de interoperabilitate, se prezumă autentice, adică se consideră integre și veridice, corespund realităților și stau la baza actelor juridice, iar furnizorii de date sunt obligați să asigure integritatea și veridicitatea acestora;

Art.7 alin.(6) Schimbul de date pentru participanții persoane fizice și juridice private are loc în bază contractuală cu respectarea prevederilor prezentei legi. Contractul de schimb de date este încheiat între deținătorul platformei de interoperabilitate și persoana fizică sau juridică privată și poate fi cu titlu oneros în cazurile prevăzute de legislație

Obiecții:

La art.1 alin.(4) proiectul prevede unele aspecte comerciale, fapt ce contravine scopului de bază enunțat. Riscul constă în faptul că, deținătorul platformei, fără cerințe bine stabilite poate furniza cu titlu oneros informații persoanelor fizice sau juridice, fără referințe la reședința acestora, inclusiv, fără a fi stabilite tipul și volumul de date, similar dacă în categoriile interesate se vor conține date cu accesibilitate limitată, sau chiar secret de stat.

Totodată, norma respectivă se află într-un conflict intern cu prevederile de la art.5 lit.a) și b) care prevede: gratuitatea datelor și respectiv accesul în egală măsură pentru toți participanții la platformă. Or, odată prestabilite posibilități de impunere a unor costuri pentru furnizarea datelor prin intermediul platformei nicidecum nu poate fi vorba despre accesul în egală măsură.

De asemenea, sintagma „*poate fi făcută contra plată*” acordă autorității competente dreptul discreționar de a decide pentru care persoane informația va fi contra cost și pentru care nu. Comportamentul abuziv și discreționar al autorității în cazul de față va fi dificil de sancționat întrucât prevederea analizată îi acordă prerogativa de interpretare.

În ceea ce privește autenticitatea datelor – nu este clar care va fi mecanismul de supraveghere și control asupra datelor din sistemele informaționale ale participanților la schimbul de date, furnizate prin intermediul platformei de interoperabilitate. Așadar, un sistem de date și informații de o așa „*anvergură*” cu un risc sporit de: *spargere, piraterie, atacuri cibernetice*, nu se poate baza pe „*buna credință*” a utilizatorilor/consumatorilor/furnizorilor. Or, persistă marele risc ca abuzând de „*prezumția*” autenticității, integrității și veridicității informației pe care o acordă norma, persoana interesată, în mod intenționat va furniza informații și date eronate urmărind scopuri coruptibile ascunse.

În sensul art.7 alin.(6) nu este clar aspectul practic de încheiere prin intermediar a contractelor de schimb de informații între furnizor și utilizator, referindu-ne la atribuțiile autorității competente, ori refuzul încheierii unor astfel de contracte fără oferirea de alternative consumatorilor nu poate reprezenta în sine activitatea de bază a unei astfel de structuri.

De asemenea, nu este clară forma și procedura de luare a deciziei din partea autorității, ținând cont de faptul că ar putea exista interese ascunse ale funcționarilor care vor gestiona sistemul, sau de protecționism pentru unii furnizori, prezumând că accesul la sursele de date din partea unor organe de control, poate duce la stabilirea neregulilor ce reies din datele utilizate (de ordin financiar, competențe ale funcționarilor, etc).

Recomandări:

La art.1 alin.(4) excluderea sintagmei „*în scopuri comerciale*”;

La art.5 excluderea sintagmei „*punerea la dispoziție a datelor deținute de participanții publici către participanți privați, poate fi făcută contra plată*”;

La art.7 alin.(6) – reglementarea posibilității de încheiere a contractului între furnizor și utilizator „*fără intermediar*”

Factori de risc:

- Concurența normelor de drept

Riscuri de corupție:

- Încurajarea sau facilitarea actelor de:

	<ul style="list-style-type: none"> • Lipsa/ambiguitatea procedurilor administrative • Atribuții excesive, improprii sau contrare statutului entității publice • Lipsa/insuficiența mecanismelor de supraveghere și control <ul style="list-style-type: none"> - corupere activă - corupere pasivă - conflict de interese și/sau favoritism • Legalizarea actelor de: <ul style="list-style-type: none"> - abuz de serviciu - depășirea atribuțiilor de serviciu - scurgere a informațiilor cu accesibilitate limitată - obținerea sau divulgarea informațiilor care constituie secret comercial, bancar sau fiscal – art.107 Cod Contravențional - obținerea ilegală și/sau divulgarea informațiilor ce constituie secret comercial sau bancar art.245/10 Cod penal - Încălcarea regulilor de securitate a sistemului informatic art.261 Cod penal - divulgarea secretului de stat art.344 Cod penal
2.	<p>Art.3 alin.(2) și art.7 alin.(3)</p> <p><u>Art.3 alin.(2) Prezenta lege se aplică de asemenea și persoanelor fizice și persoanelor juridice private, în măsura în care acestea dețin sisteme informaționale, dispun de date ce prezintă interes pentru autoritățile și instituțiile publice sau pentru alte persoane fizice și persoane juridice private, și își manifestă disponibilitatea și intenția de a participa la schimbul de date în conformitate cu prezenta lege.</u></p> <p><u>Art.7 alin.(3) Autoritățile și instituțiile publice, persoanele juridice fondate sau gestionate de autorități și instituții publice, precum și persoanele juridice private, care în numele autorităților și instituțiilor publice sau persoanelor juridice fondate sau gestionate de autorități și instituții publice, care gestionează sau dețin sisteme informaționale sunt obligate să asigure schimbul de date prin intermediul platformei de interoperabilitate și nu pot invoca motive de ordin tehnic sau organizatoric pentru a refuza direct sau indirect schimbul de date cu excepția cazurilor prevăzute de lege.</u></p> <p>Obiecții:</p> <p>Sintagma „<i>și își manifestă disponibilitatea și intenția de a participa la schimbul de date în conformitate cu prezenta lege</i>” de la art.3 alin.(2) se află în conflict intern de norme cu prevederea de la art.7 alin.(3) care reglementează că, „<i>sunt obligate să asigure schimbul de date prin intermediul platformei de interoperabilitate</i>”</p> <p><i>Totodată, sintagma „și nu pot invoca motive de ordin tehnic sau organizatoric pentru a refuza direct sau indirect schimbul de date cu excepția cazurilor prevăzute de lege”, impune cerințe excesive pentru realizarea drepturilor/obligațiilor în sensul în care, multe autorități publice dispun de sisteme informaționale aflate în exploatare care au fost proiectate anterior, fără a lua în considerație principiile actuale de interoperabilitate sau au fost realizate în baza contractelor sau acordurilor bilaterale existente de schimb de date încheiate direct între participanți ceea ce face dificilă dacă nu chiar imposibilă ajustarea sistemelor informaționale existente la platforma de interoperabilitate.</i></p> <p>De asemenea, instituirea unei obligații de furnizare a informațiilor doar prin platforma de interoperabilitate îngreșează dreptul de acces liber la informație și de a alege sursa de informare în contextul în care platforma de interoperabilitate reprezintă doar una din posibilitățile tehnice de furnizare a informației.</p> <p>Așadar, norma creează premise pentru aplicarea abuzivă a prevederilor din proiect și face astfel dificilă atragerea la răspundere a persoanelor responsabile, acestea din urmă profitând de caracterul interpretativ al normelor.</p>

	<p>Recomandări: Substituirea sintagmei „sunt obligate să asigure schimbul de date prin intermediul platformei de interoperabilitate și nu pot invoca motive de ordin tehnic sau organizatoric pentru a refuza direct sau indirect schimbul de date cu excepția cazurilor prevăzute de lege” cu sintagma „pot asigura schimbul de date prin intermediul platformei de interoperabilitate”.</p> <table border="1" data-bbox="282 358 1500 659"> <tr> <td data-bbox="282 358 817 659"> <p>Factori de risc:</p> <ul style="list-style-type: none"> ● Concurența normelor de drept ● Atribuții care admit derogări și interpretări abuzive ● Limitarea neîntemeiată a drepturilor omului ● Cerințe excesive pentru realizarea drepturilor/obligații excesive </td> <td data-bbox="817 358 1500 659"> <p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● Legalizarea actelor de: <ul style="list-style-type: none"> - Abuz de serviciu - Depășire a atribuțiilor de serviciu </td> </tr> </table>	<p>Factori de risc:</p> <ul style="list-style-type: none"> ● Concurența normelor de drept ● Atribuții care admit derogări și interpretări abuzive ● Limitarea neîntemeiată a drepturilor omului ● Cerințe excesive pentru realizarea drepturilor/obligații excesive 	<p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● Legalizarea actelor de: <ul style="list-style-type: none"> - Abuz de serviciu - Depășire a atribuțiilor de serviciu
<p>Factori de risc:</p> <ul style="list-style-type: none"> ● Concurența normelor de drept ● Atribuții care admit derogări și interpretări abuzive ● Limitarea neîntemeiată a drepturilor omului ● Cerințe excesive pentru realizarea drepturilor/obligații excesive 	<p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● Legalizarea actelor de: <ul style="list-style-type: none"> - Abuz de serviciu - Depășire a atribuțiilor de serviciu 		
3.	<p>Art.7, alin.(1) și alin.(5), art.12 alin.(2) și art.13 alin.(4) și alin.(9)</p> <p>Articolul 7.</p> <p>Alin.(1) Platforma de interoperabilitate se instituie de către Guvern,</p> <p>Alin.(5) Schimbul de date între sistemele informaționale deținute de același participant public, poate avea loc și în afara platformei de interoperabilitate.</p> <p>Art.12. alin.(2) Conectarea la platforma de interoperabilitate a participanților deținători ai sistemelor informaționale ale altor state are loc doar prin <u>autorizarea prealabilă</u> de către <u>Autoritatea competentă</u> și Centrul Național pentru Protecția Datelor cu Caracter Personal pentru setul de date respectiv.</p> <p>Art.13. alin.(4) Participantul la schimbul de date poartă răspundere pentru lipsa notificării în <u>adresa Autorității competente</u>, privind limitarea mandatului sau schimbarea condițiilor sau atribuțiilor sale legale, și respectiv limitarea setului de date.</p> <p>Alin.(9) <u>Controlul respectării cerințelor prezentei legi se efectuează de către Autoritatea competentă</u> de comun cu Centrul Național pentru Protecția Datelor cu Caracter Personal pentru setul de date respectiv.</p> <p>Obiecții</p> <p>La alin.(1) art.7 din proiect, se atrage atenția supra faptului că platforma de interoperabilitate a fost aprobată prin Hotărârea Guvernului nr.404/2014 cu privire la pilotarea platformei de interoperabilitate, iar prin pct.2 din hotărârea menționată „Se desemnează:</p> <p>„1) Cămară de Stat în calitate de posesor al platformei de interoperabilitate;</p> <p>2) Centrul de Guvernare Electronică (E-Government) în calitate de deținător al platformei de interoperabilitate;</p> <p>3) Întreprinderea de Stat “Centrul de telecomunicații speciale” în calitate de operator tehnico-tehnologic al platformei de interoperabilitate.</p> <p>3. Se stabilește perioada de pilotare a platformei de interoperabilitate până la data de 31 decembrie 2018.”</p> <p>În sensul art.12 alin.(2) din proiect nu este clară procedura de „<u>autorizare prealabilă</u>” de către Autoritatea competentă. Or, conform Legii nr.133/2011, autorizarea pentru accesare, prelucrare și utilizare a informațiilor ce conțin date cu caracter personal este competența exclusivă a CNPDCP. Astfel nu este</p>		

cazul intermedierei acestei proceduri prin o „*autorizare prealabilă*” de către Autoritatea competentă.

Totodată se menționează că întru realizarea mai bună a competențelor de prevenirea și combaterea criminalității, asigurarea ordinii publice, apărarea drepturilor și intereselor legitime ale persoanelor, este necesară instituirea unui cadru legislativ adecvat, instituțional funcțional și capabil să răspundă la necesitățile reale ale organelor de drept în calitate de deținători de date și participanți la sistem.

Se reiterează că, rezultatele obținute în urma pilotării Platformei de interoperabilitate, la care au participat câteva instituții publice, nu au devenit cunoscute majorității utilizatorilor de date, în mod special, organelor din domeniul apărării naționale, securității statului și ordinii publice, catalogați la nivel național drept cei mai mari consumatori de date cu regim juridic special, din acest motiv se consideră că este prematur de a ne expune despre legalizarea funcționării unui sistem lipsit în prezent de „*materia primă*” (*informație*) necesară, care în același timp se obligă artificial de a răspunde la cerințele consumatorilor, suplimentar incluzând și reguli de control lipsite de mecanisme ordonate de lucru.

De asemenea, prezentul proiect vine să excludă unele norme cu caracter restricționat prevăzute în art. 15 și art. 24 alin.(4) din Legea nr. 133/2011 privind protecția datelor cu caracter personal, elemente ce vor provoca conflicte de norme la implementarea art. 7, 8, 12 și 13 din actual proiect.

Astfel, conform art.15 al Legii nr.133/2011 „(1) Prevederile art.4 alin.(1), art.12 alin.(1) și (2), art.13, 14 și 28 nu se aplică în cazul în care prelucrarea datelor cu caracter personal este efectuată în cadrul acțiunilor prevăzute la art.2 alin.(2) lit.d), în scopul apărării naționale, al securității statului și menținerii ordinii publice, al protecției drepturilor și libertăților subiectului datelor cu caracter personal sau ale altor persoane, dacă prin aplicarea acestora este prejudiciată eficiența acțiunii sau obiectivul urmărit în exercitarea competențelor legale ale autorității publice.”

În acest context se consideră imperios a se păstra excepțiile actuale din Legea nr.133/2011, acest fapt fiind important din considerentul că restricțiile ce țin de contractarea accesului la sursele de date sunt de durată, în același timp, sunt contrar intereselor utilizatorilor actuali din cadrul CNA, ținând cont de riscurile sporite de scurgerea informațiilor la etapa de investigare a infracțiunilor până la pornirea urmăririi penale.

Potrivit argumentelor aduse de inițiator la susținerea proiectului de lege, se operează cu noțiuni de Clasificatoare și Cataloage, care până în prezent nu au fost elaborate, fapt ce creează confuzii în jurul acestor expresii și mari inexactități la percepția categoriilor de date care se vor include în platformă, la fel ca imposibilitatea identificării furnizorilor și participanților de drept, precum și gradul de participare al acestora la funcționarea sistemului. De exemplu, nu este clar dacă deținătorii de date din domeniul bancar sau operatorii de telecomunicații se vor regăsi în platforma respectivă, iar accesul la date care se face în prezent pe bază de mandat în cadrul procesului penal se va face sau nu prin intermediul autorității competente, ceea ce în prezent unele atribuții le aparține Serviciului de Informații și Securitate.

În ceea ce privește art.13 alin.(4) acesta contravine Legii nr.133/2011 care prevede că: “(1) *Operatorii sânt obligați să notifice Centrul, personal sau prin persoanele împuternicite de către ei, înainte de a prelucra date cu caracter personal destinate să servească unui scop. Prelucrarea altor categorii de date cu caracter personal decât cele notificate anterior se va efectua cu condiția unei noi notificări.”*

De asemenea conform Legii nr.133/2011 atribuțiile de control revin tot CNPDCP.

În acest context, este dificilă identificarea mecanismului de sancționare a persoanelor responsabile de aplicarea abuzivă a normelor care generează acțiuni cu caracter corupțional.

Recomandarea:

La art.7 - Expunerea alin. (5) după cum urmează: „Schimbul de date între sistemele informaționale deținute de același participant public, precum și în cazurile de solicitare a accesului la informații de către Centrul Național Anticorupție în scopul efectuării investigațiilor și/sau analizei operaționale și strategice a actelor de corupție, a actelor conexe corupției și a faptelor de comportament corupțional, a studiilor analitice ale fenomenului corupției, poate avea loc și în afara platformei de interoperabilitate.”

La art.12 alin.(2) și art.13 alin.(9) excluderea sintagmei „Autoritatea competentă”
 La art.13 alin.4 substituirea sintagmei “autoritatea competentă” cu sintagma “Centrul Național pentru Protecția Datelor cu Caracter Personal”

Factori de risc:

- Concurența normelor de drept
- Lipsa ambiguitatea procedurilor administrative
- Atribuții excesive, improprii sau contrare statutului entității publice

Riscuri de corupție:

- **Încurajarea sau facilitarea actelor de:**
 - scurgere a informațiilor cu accesibilitate limitată
- **Legalizarea actelor de:**
 - conflict de interese și/sau favoritism
 - abuz de serviciu
 - depășire a atribuțiilor de serviciu

4. Art.7 alin.(9), (10), (11), (12) și (14)

(9) Furnizorul de date este în drept să refuze orice solicitare de schimb de date în afara platformei de interoperabilitate, dacă acesta sau deținătorul platformei de interoperabilitate pune la dispoziția consumatorului de date, o interfață de schimb de date prin intermediul platformei de interoperabilitate.

(10) Participanții la schimbul de date sunt obligați să asigure în mod constant resursele (umane, financiare, tehnologice, etc.) și să întreprindă măsurile necesare, inclusiv recomandate de Autoritatea competentă, pentru asigurarea conectării și continuității schimbului de date.

(11) La examinarea cererilor de conectare la platforma de interoperabilitate, Autoritatea competentă verifică respectarea de către participanți a prevederilor legislației, inclusiv a legislației privind accesul la informațiile cu accesibilitate limitată și a legislației privind protecția datelor cu caracter personal în mod special. Autoritatea competentă poate cere dovada privind dreptul de acces la informația respectivă. Anterior conectării la platforma de interoperabilitate, Autoritatea competentă verifică existența autorizării prelucrărilor de date cu caracter personal emise de Centrul Național pentru Protecția Datelor cu Caracter Personal în condițiile legislației privind protecția datelor cu caracter personal. În lipsa autorizării conectarea la platforma de interoperabilitate este interzisă pentru setul de date respectiv.

(12) Evenimentele legate de schimbul de date sunt jurnalizate. Modul și procedura de jurnalizare și acces la informația jurnalizată sunt stabilite de către Guvern. [...]

(14) În procesul testării conectării și integrării sistemelor informaționale, accesarea datelor cu caracter personal de către Autoritatea competentă sau solicitant, prin intermediul platformei de interoperabilitate, nu necesită consimțământul subiectului de date cu caracter personal

Obiecții

La alin.(9) În condițiile în care, va exista o interfață separată pentru încărcarea datelor inițiale și pentru tranzacțiile curente punerea la dispoziția consumatorului de date, o interfață de schimb de date prin intermediul platformei de interoperabilitate prezintă riscul scurgerii de informații și accesului ilegal la informații ce constituie secret de stat, bancar sau comercial precum și la datele cu caracter personal.

Norma de la alin.(10) obligă participanții la schimbul de date să asigure în mod constant resursele (umane, financiare, tehnologice, etc.) și să întreprindă măsurile necesare, inclusiv recomandate de Autoritatea competentă, pentru asigurarea conectării și continuității schimbului de date.

Astfel, nu este clar mecanismul de aplicare și impunere a normelor respective în condițiile în care din start se impun cerințe excesive pentru realizarea drepturilor/obligățiilor. Or, conform art.4 din proiect, participant la schimbul de date, participanți la schimbul de date – sunt: „*autorități și instituții publice, persoane juridice fondate sau gestionate de autorități și instituții publice, precum și persoane juridice private, care în numele autorităților și instituțiilor publice sau persoanelor juridice fondate sau gestionate de autorități și instituții publice, care gestionează sau dețin sisteme informaționale. În calitate de participanți pot fi și persoanele fizice și persoanele juridice de drept privat, rezidenți ai Republicii Moldova, în măsura în care acestea își manifesta intenția de a participa benevol la schimbul de date și nu sunt utilizatori de informație.*”

Referitor la alin.(11) se atestă o neconcordanță a acestuia cu prevederile art.4 alin.(2) al Legii nr.780/2001 privind actele legislative, care stipulează că: „actul legislativ trebuie să corespundă dispozițiilor constituționale și să fie în concordanță cu cadrul juridic existent, cu sistemul de codificare și unificare a legislației.”

Sintagma „autoritatea competentă poate cere dovada privind dreptul de acces la informația respectivă”, acordă acestei Autorități dreptul de a decide la propria discreție cazurile în care va cere dovada și care nu, decizia fiind influențată în dependență de interesul coruptibil al acesteia.

Totodată, norma se află în conflict și cu prevederile de la lit.a) alin.(3) art.4 din Legea nr.780/2011 care reglementează principiul oportunității, coerenței, consecvenței și echilibrului între reglementările concurente. Or, în procesul de legiferare, respectarea tuturor cerințelor impuse de legea sus numită este primordială.

De asemenea, nu este argumentată necesitatea ca Autoritatea competentă să fie intermediar între participanții la platformă și CNPDCP.

În sensul alin.(12) nu este clară noțiunea de „jurnalizare a informației” și „jurnalizare a schimbului de date.” Or, unul din obiectivele proiectului de lege supus expertizei este excluderea deținerii manuale a registrelor. Astfel este important a se specifica expres ce se are în vedere prin „jurnalizare a informațiilor”.

În ceea ce privește alin.(14) este necesar a se face trimitere la art.5 alin.(5), din Legea nr.133/2011 privind protecția datelor cu caracter personal, care prevede exhaustiv cazurile în care consimțământul subiectului datelor cu caracter personal nu este necesar.

Totodată, conform art.19 alin.(1) al aceluiași act legislativ se menționează că, „Controlul asupra conformității prelucrării datelor cu caracter personal cu cerințele prezentei legi se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter Personal, (în continuare CNPDCP) care acționează în condiții de imparțialitate și independență.”

Deficiențele normelor analizate, creează premise de aplicare abuzivă de către persoanele responsabile, fiind dificilă atragerea la răspundere a acestora întrucât norma „aparent” ar permite un asemenea comportament.

Recomandări:

Excluderea alin.(9), (10) și (11) (14)

Includerea la art.4 a noțiunii de „jurnalizare a datelor” și definirea acesteia

Factori de risc:

- Atribuții excesive, improprii sau contrare statutului entității publice
- Concurența normelor de drept
- Lipsa/insuficiența mecanismelor de supraveghere și control
- Lipsa/ambiguitatea procedurilor

Riscuri de corupție:

- Încurajarea sau facilitarea actelor de:
 - scurgere a informațiilor cu accesibilitate limitată
- Legalizarea actelor de:
 - conflict de interese și/sau favoritism
 - abuz de serviciu
 - depășire a atribuțiilor de serviciu

	administrative ● Introducerea termenilor noi care nu au o definiție în legislație sau în proiect
5.	<p>Art.8</p> <p><u>Art.8 alin.(1) Autoritatea competentă pentru asigurarea schimbului de date și interoperabilității este organul desemnat de către Guvern, care, în conformitate cu prezenta lege, asigură interoperabilitatea semantică și stabilește principiile interoperabilității tehnice și organizatorice.</u></p> <p><u>Alin.(2) Autoritatea competentă are următoarele împuterniciri și atribuții:</u></p> <p>a) <u>examinează, acceptă sau respinge, în termen de cel mult 30 de zile, solicitările de conectare la platforma de interoperabilitate primite din partea participanților la schimbul de date;</u></p> <p>b) <u>emite decizii privind acceptarea sau respingerea solicitărilor de conectare la platforma de interoperabilitate primite din partea participanților la schimbul de date;</u></p> <p>c) <u>administrează Catalogul semantic inclusiv identifică, înregistrează, publică, actualizează și elimină active semantice;</u></p> <p>d) <u>stabilește autoritățile responsabile de deținerea și dezvoltarea activelor semantice conform domeniilor de competență ale acestora, precum și sursele de date asociate acestor active;</u></p> <p>e) <u>aprobă condițiile tehnice standard și modelul contractului privind utilizarea platformei de interoperabilitate;</u></p> <p>f) <u>solicită conectarea autorităților și instituțiilor publice, persoanelor juridice fondate sau gestionate de autorități și instituții publice, precum și persoanelor juridice private, care în numele autorităților și instituțiilor publice sau persoanelor juridice fondate sau gestionate de autorități și instituții publice, care gestionează sau dețin sisteme informaționale, la platforma de interoperabilitate cu scopul consumului sau furnizării de date;</u></p> <p>g) <u>suspendă sau decide asupra deconectării, din oficiu sau la solicitarea organelor competente, utilizarea platformei de interoperabilitate de către un participant la schimbul de date în cazurile nerespectării condițiilor tehnice și a prevederilor prezentei legi, precum și la solicitarea participantului în cazurile prevăzute de legislație;</u></p> <p>h) <u>monitorizează implementarea politicilor publice în domeniul schimbului de date și a interoperabilității;</u></p> <p>i) <u>examinează, inclusiv în comun cu alte autorități abilitate, cazurile de cooperare transfrontalieră în domeniul schimbului de date și a interoperabilității;</u></p> <p>Obiecții:</p> <p>Raportând norma analizată la art.20 din Legea nr.133/2011 care prevede atribuțiile CNPDCP, se constată că atribuțiile acordate Autorității competente, din proiect sunt întocmai ca atribuțiile descrise de legea nr.133/2011. Astfel, nu este clară necesitatea instituirii unei Autorități care doar ar dubla competențele, atribuțiile și drepturile unei autorități deja existente și funcționale.</p> <p>Riscul coruptibil rezidă din faptul că atribuțiile paralele generează conflicte de competență sau declinări de competență între ambele entități responsabile. Astfel, atunci când pentru una și aceeași decizie, acțiune, inacțiune sunt responsabile două entități diferite este dificil a identifica care anume entitate se face vinovată, astfel că atragerea la răspundere pentru actele coruptibile abuz și discreții va fi mai mult decât dificilă.</p> <p>Totodată, dublarea de competențe pentru un domeniu care necesită precauție și vigilență pecum este gestionarea sistemului de informații și baze de date, inclusiv secrete, încurajează/facilitează scurgerea de informații, cât și realizarea altor acțiuni coruptibile care au legătură cu informația respectivă.</p>

	<p>Recomandarea: Excluderea art.8</p> <p>Factori de risc:</p> <ul style="list-style-type: none"> ● Concurența normelor de drept ● Atribuții excesive, improprii sau contrare statutului entității publice ● Atribuții paralele ● Cumularea competențelor de a stabili rigori, a controla aplicarea lor și de a sancționa <p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● Încurajarea sau facilitarea actelor de: <ul style="list-style-type: none"> - corupere pasivă - corupere activă - conflict de interese și/sau favoritism - scurgere a informațiilor cu accesibilitate limitată ● Legalizarea actelor de: <ul style="list-style-type: none"> - abuz de serviciu - depășirea atribuțiilor de serviciu
6.	<p>Art.9</p> <p>(1) <u>Securitatea și confidențialitatea schimbului de date este asigurată de către toți participanții la schimbul de date și deținătorul platformei pe domeniul lor de competență și în conformitate cu cerințele de securitate aplicate pentru categoria respectivă de date.</u></p> <p>(2) Pentru asigurarea confidențialității schimbului de date și accesării informației cu accesibilitate limitată, platforma de interoperabilitate <u>asigură posibilitatea transportării datelor în formă criptată. Criptarea și decriptarea datelor este asigurată de către furnizorul de date și corespunzător consumatorul de date.</u></p> <p>Obiecții:</p> <p>În contextul în care, proiectul de lege, are drept scop facilitarea schimbului de date în sectorul public și asigurarea securității informaționale, în prevederile acestuia nu se regăsesc norme suficiente și clare ce ar spori securitatea informației, ba din contra, responsabilitatea dată este pusă în sarcina participanților la schimbul de date și nu a autorității competente, după cum se indică în alin. (1) art. 9 din proiect. Or, nefiind stabilite expres cerințele de securitate, categoriile de date pe care le dețin participanții la platformă cât și mecanismul clar de asigurare a securității informaționale, duce la vulnerabilizarea sectorului informațional ceea ce poate afecta în egală măsură atât sectorul economico-financiar cât și sectorul securității statului.</p> <p><u>Sintagma "Securitatea și confidențialitatea schimbului de date este asigurată de către toți participanții la schimbul de date"</u> include în sine un cerc mult prea larg de subiecți la care se referă prevederea și deci acest fapt face dificilă atragerea la răspundere a persoanelor care vor utiliza abuziv informațiile și datele prin intermediul platformei de interoperabilitate.</p> <p>Totodată, potrivit actualelor tehnici IT, transportarea datelor la distanță este obligatoriu protejată prin diverse mecanisme de criptare a datelor, și nu se resimte necesitatea de <u>intermediere</u> prin platforma de interoperabilitate, care prin influența factorului uman poate deveni un izvor important de scurgeri de informații, indiferent de modul de criptate, dat fiind faptul că, fluxul de transmitere va fi centralizat într-un singur sistem, mult mai ușor de controlat prin registrul cererilor (accesărilor) în sistem. În prezent scurgeri de date la acest nivel sunt excepții, și pot fi ușor documentate în caz de identificare a acestora.</p> <p>În condițiile în care, mecanismul de protecție folosit de un sistem pentru a transmite mesaje depinde de o multitudine de factori cu ar fi: complexitatea sistemului, resursele disponibile, gradul de importanță și criteriul de secretizare a informației care urmează a fi protejată, precum și celelalte sisteme cu care interacționează, nu este clar care va fi mecanismul de asigurare a confidențialității informației prin transportarea datelor în formă criptată cât și care formă de criptare va fi folosită: criptarea simetrică, sau criptarea asimetrică.</p> <p>În acest sens, urmează a se lua în calcul că problema cea mai importantă în sistemul de criptare, este <u>păstrarea secretului cheilor folosite</u> și transferul acestora între utilizatori. Or, deconspirarea acestora duce la compromiterea sistemelor de criptare folosite.</p>

	<p>Astfel, nu este clar, în sarcina căreia autorități sau parte la platformă se va pune securitatea cheilor și cum se va monitoriza manipularea acestora pentru decodificarea informațiilor criptate și cine va gestiona aceste chei.</p> <p>De asemenea, procesul de criptare și decriptare a informației presupune în sine un întreg sistem tehnologico-informațional care necesită un grad înalt de profesionalism și vigilență fiind necesare crearea cheilor publice și cheilor private pentru codificare și decodificarea informațiilor criptate. Cheile de criptare sunt stocate pe calculator. O cheie publică poate fi cunoscută și utilizată de către toți participanții la platformă pe când o cheie privată este accesibilă doar prin intermediul unei parole. Dacă parola a fost uitată ori dacă din ne atenție a fost șters fișierul aferent cheilor de criptare, nu mai pot fi decriptate datele la care se pretau cheile pierdute ori inaccesibile.</p> <p>Astfel, nu este clar cine va crea, elibera, gestiona, monitoriza manipularea cheilor respective precum și cine va suporta cheltuielile financiare pentru acțiunile date. Or, odată cu evoluția, avansarea și modernizarea tehnologiilor informaționale apare necesitatea de securizare strictă a sectorului respectiv, iar normele din proiect nu asigură nici pe departe garanția evitării unor atacuri cibernetice. Or, de multe ori, o manipulare în cadrul unui atac cibernetic, poate nu doar să intercepteze mesajele, dar poate să le și modifice, să le șteargă, să le scurteze, să le substituie, ceea ce compromite din capul locului prevederile referitoare la integritatea informațiilor, corectitudinea și exactitatea acestora. Dificultatea asigurării unui sistem împotriva unor astfel de atacuri devine mult mai dificilă, și stă la baza întregului domeniu al criptanalizei.</p> <p>De notat că, în prezent rolul de control al resurselor informaționale importante pentru stat revine Serviciului de Informații și Securitate, conform prevederilor art. 7 lit. b) din Legea nr. 753 din 23.12.1999 - <i>protecția secretului de stat, exercitarea controlului privind asigurarea păstrării și prevenirii scurgerii informațiilor ce constituie secret de stat și altor informații importante pentru stat.</i></p> <p>Așadar, stocarea tuturor informațiilor într-o singură sursă informațională constituie un risc major ca aceste informații să fie accesate/utilizate în alte scopuri decât cele stabilite de cadrul normativ, iar modalitatea și mecanismul de securizare acestora nu este reflectat în prevederile analizate. În consecință, acest fapt va duce la dificultatea sau chiar imposibilitatea sancționării persoanelor responsabile de acțiunile abuzive, întrucât caracterul interpretativ al normei „aparent” acordă acesteia dreptul de a aplica prevederea la propria discreție.</p> <p>Recomandări:</p> <p>La alin.(1) art.8 - Identificarea unui singur subiect care va asigura confidențialitatea și securitatea datelor și informațiilor care circulă prin intermediul platformei de interoperabilitate.</p> <p>La alin.(2) art.8 - Completarea normei cu prevederi care ar face referire la: categoriile de criptare care urmează a fi utilizate (simetrică, asimetrică, convențională etc.), deținătorii cheilor de criptare, cine va crea, elibera, gestiona, monitoriza manipularea cheilor respective precum și cine va suporta cheltuielile financiare pentru acțiunile respective.</p> <table border="1" data-bbox="267 1560 1474 1911"> <tr> <td data-bbox="267 1560 803 1911"> <p>Factori de risc:</p> <ul style="list-style-type: none"> ● Cerințe excesive pentru realizarea drepturilor/Obligații excesive ● Norme irealizabile ● Nedeterminarea entității publice responsabile la care se referă prevederea ● Lipsa/ambiguitatea procedurilor administrative ● Lipsa/insuficiența mecanismelor de supraveghere și control </td> <td data-bbox="803 1560 1474 1911"> <p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● - Încurajarea sau facilitarea actelor de: - scurgere a informațiilor cu accesibilitate limitată ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu </td> </tr> </table> <p>7. Art.10 alin.(2) Art.10 alin.(2) În scopul asigurării calității adaptării și identificării datelor autentice, la adaptarea datelor, platforma de interoperabilitate poate accesa de la furnizorii de date un set de date mai mare decât cel solicitat de către consumatorul de date. Accesarea cu scopul adaptării, a setului</p>	<p>Factori de risc:</p> <ul style="list-style-type: none"> ● Cerințe excesive pentru realizarea drepturilor/Obligații excesive ● Norme irealizabile ● Nedeterminarea entității publice responsabile la care se referă prevederea ● Lipsa/ambiguitatea procedurilor administrative ● Lipsa/insuficiența mecanismelor de supraveghere și control 	<p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● - Încurajarea sau facilitarea actelor de: - scurgere a informațiilor cu accesibilitate limitată ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu
<p>Factori de risc:</p> <ul style="list-style-type: none"> ● Cerințe excesive pentru realizarea drepturilor/Obligații excesive ● Norme irealizabile ● Nedeterminarea entității publice responsabile la care se referă prevederea ● Lipsa/ambiguitatea procedurilor administrative ● Lipsa/insuficiența mecanismelor de supraveghere și control 	<p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● - Încurajarea sau facilitarea actelor de: - scurgere a informațiilor cu accesibilitate limitată ● Legalizarea actelor de: - abuz de serviciu - depășire a atribuțiilor de serviciu 		

	<p><u>de date care nu a fost transmis consumatorului de date, nu se consideră consum de date de către deținătorul platformei de interoperabilitate.</u></p> <p>Obiecții: Sistemul de gestionare a bazei de date fiind un produs software furnizat de producătorul bazei de date, trebuie să pună la dispoziție toate serviciile de bază necesare pentru organizarea și întreținerea bazei de date, cum ar fi: transferarea datelor în/și din fișierele fizice de date, în funcție de cerințe; gestionarea accesului concurențial la date al mai multor utilizatori, inclusiv prevenirea conflictelor care ar putea fi cauzate de actualizările simultane; gestionarea tranzacțiilor, astfel încât toate modificările făcute asupra bazei de date printr-o tranzacție să fie executate ca o singură unitate; acceptarea un limbaj de interogare; adaptarea unor funcții pentru salvarea bazei de date și pentru refacerea bazei de date în urma erorilor; mecanisme de securitate pentru împiedicarea accesului neautorizat la date și modificarea acestora.</p> <p>Astfel, adaptarea datelor trebuie să fie efectuată instantaneu, din momentul introducerii acestora în sistemul de platformă, nefiind necesară o procedură de adaptare aparte. Or, în cazul de față, sub pretextul adaptării datelor persoana responsabilă care are acces la platforma de interoperabilitate va accesa un set de date mai mare, în funcție de interesul urmărit și nu va putea fi atras la răspundere pentru accesarea/ulterior utilizarea acestor date, întrucât norma îi permite acest comportament.</p> <p>Recomandarea: Excluderea alin.(2) de la art.10</p> <table border="0" data-bbox="256 869 1482 1137"> <tr> <td data-bbox="256 869 790 1137"> <p>Factori de risc:</p> <ul style="list-style-type: none"> ● Atribuții excesive, improprii sau contrare statutului entității publice ● Lipsa/insuficiența mecanismelor de supraveghere și control </td> <td data-bbox="790 869 1482 1137"> <p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● Legalizarea actelor de: <ul style="list-style-type: none"> - abuz de serviciu - depășirea atribuțiilor de serviciu - scurgerea informațiilor cu accesibilitate limitată - obținerea sau divulgarea informațiilor care constituie secret comercial, bancar sau fiscal – art.107 Cod Contravențional </td> </tr> </table>	<p>Factori de risc:</p> <ul style="list-style-type: none"> ● Atribuții excesive, improprii sau contrare statutului entității publice ● Lipsa/insuficiența mecanismelor de supraveghere și control 	<p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● Legalizarea actelor de: <ul style="list-style-type: none"> - abuz de serviciu - depășirea atribuțiilor de serviciu - scurgerea informațiilor cu accesibilitate limitată - obținerea sau divulgarea informațiilor care constituie secret comercial, bancar sau fiscal – art.107 Cod Contravențional
<p>Factori de risc:</p> <ul style="list-style-type: none"> ● Atribuții excesive, improprii sau contrare statutului entității publice ● Lipsa/insuficiența mecanismelor de supraveghere și control 	<p>Riscuri de corupție:</p> <ul style="list-style-type: none"> ● Legalizarea actelor de: <ul style="list-style-type: none"> - abuz de serviciu - depășirea atribuțiilor de serviciu - scurgerea informațiilor cu accesibilitate limitată - obținerea sau divulgarea informațiilor care constituie secret comercial, bancar sau fiscal – art.107 Cod Contravențional 		
8.	<p><u>Art.13 alin.(4)</u> <u>Art.13 alin.(4) Participantul la schimbul de date poartă răspundere pentru lipsa notificării în adresa Autorității competente, privind limitarea mandatului sau schimbarea condițiilor sau atribuțiilor sale legale, și respectiv limitarea setului de date.</u></p> <p>Obiecții: Realizarea schimbului de date prin intermediul platformei de interoperabilitate presupune accesul la o bază de date care constituie în sine toată informația necesară pentru buna desfășurare a relațiilor/raporturilor juridice care au tangență cu sistemele informaționale. În această ipoteză, acordarea dreptului de a primi notificările precum și alte atribuții de supraveghere, control etc, unei „Autorități” dublează efectiv competențele și atribuțiile CNPDCP. În acest context, autoritatea competentă își atribuie competențe care de fapt și de drept aparțin unei alte autorități. Or, conform dispozițiilor Legii nr.133/2011, CNPDCP este autoritatea care cade sub incidența notificării.</p> <p>În acest sens, se remarcă faptul că dublarea de competențe nu va acorda un plus valoare siguranței și bunei desfășurări a schimbului de date și interoperabilitate, ci doar va genera cazuri de abuzuri, scurgeri de informații și va face dificilă atragerea la răspundere a persoanelor vinovate de realizarea acțiunilor respective, întrucât va fi dificilă identificarea acestora.</p> <p>Totodată, conform art.23 alin.(1) al Legii nr.133/2011 privind protecția datelor cu caracter personal, „Operatorii sânt obligați să notifice Centrul, personal sau prin persoanele împuternicite de către ei, înainte de a prelucra date cu caracter personal destinate să servească unui scop. Prelucrarea altor categorii de date cu caracter personal decât cele notificate anterior se va efectua cu condiția unei noi notificări.”</p> <p>Recomandarea: Substituirea sintagmei “Autorității competente” cu sintagma “Centrului Național pentru Protecția Datelor</p>		

<i>cu Caracter Personal.”</i>	
Factori de risc: <ul style="list-style-type: none"> ● Concurența normelor de drept ● Atribuții excesive, improprii sau contrare statutului entității publice ● Nedeterminarea entității publice responsabile/subiectului la care se referă prevederea ● Atribuții paralele 	Riscuri de corupție: <ul style="list-style-type: none"> ● Încurajarea sau facilitarea actelor de: <ul style="list-style-type: none"> - scurgerea informațiilor cu accesibilitate limitată - obținerea sau divulgarea informațiilor care constituie secret comercial, bancar sau fiscal – art.107 Cod Contravențional ● - Legalizarea actelor de: <ul style="list-style-type: none"> - abuz de serviciu - depășirea atribuțiilor de serviciu

IV. Concluzia expertizei

Proiectul a fost elaborat de către Cancelaria de Stat cu scopul implementării cadrului de interoperabilitate guvernamental a sistemelor informaționale de stat, prin instituirea bazei juridico-normative pentru utilizarea platformei de interoperabilitate, care ar reglementa procesul de schimb de date prin interconectarea și interoperabilitatea conținutului/resurselor informaționale și procedura de acordare a accesului la registrele și bazele de date de importanță națională pentru toate entitățile din sectorul public, în conformitate cu competențele lor legale și în scopurile conforme legii.

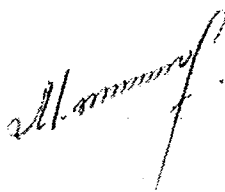
Analizând prevederile proiectului se constată că scopul declarat de către autor în nota informativă nu corespunde scopului real al proiectului care este „*facilitarea schimbului de date și interoperabilitatea, atât în scopuri comerciale, cât și necomerciale.*”

Astfel se atestă o neconcordanță între scopul declarat în nota informativă și prevederile proiectului. Or, instituirea unei platforme de interoperabilitate și obligarea prin lege a tuturor consumatorilor și furnizorilor de date să accedă la platforma respectivă cu posibilitatea instituirii unor taxe pentru acest fapt constituie un abuz din partea legiuitorilor și manifestă dubii asupra scopului „nobil” al proiectului. Astfel că, acordarea posibilității de impunere a taxelor pentru furnizarea informației se atestă ca încercarea monopolizării sectorului informațional în servirea scopului financiar a anumitor persoane sau grupuri de interese.

Prevederile proiectului conțin carențe care ar putea facilita abuzuri și discreții la aplicare. Prin proiect se urmărește instituirea unei autorități suplimentare cu funcții de control, al cărei mecanism de lucru nu este reglementat, la fel și consecințele ce se vor răsfrânge asupra deținătorilor de date ca urmare a presupuselor încălcări stabilite în rezultatele controalelor efectuate de aceasta, eventualele sancțiuni și penalități, etc.

Totodată implementarea prevederilor proiectului fără a înlătura deficiențele depistate și analizate în prezentul Raport de expertiză, va legaliza, încuraja sau facilita abuzuri, discreții și alte manifestări cu caracter coruptibil, precum și scurgerea informațiilor cu accesibilitate limitată ceea ce ar putea afecta atât securitatea statului la general, cât și securitatea datelor cu caracter personal în special.

25 august 2017



Experti ai Direcției legislație și expertiză anticorupție:
Vera Macovei, inspector