PROIECT

H O T Ă R Â R E
pentru aprobarea soluției de ”ghișeu unic” pentru implementarea resursei informaționale în domeniul comerțului

nr. _____ din _____

În vederea realizării Strategiei naţionale de dezvoltare „Moldova 2020”, aprobate prin Legea nr.166 din 11 iulie 2012 (Monitorul Oficial al Republicii Moldova, 2012, nr.245-247, art.791), cu modificările şi completările ulterioare, şi a Strategiei reformei cadrului de reglementare a activităţii de întreprinzător pentru anii 2013-2020, aprobate prin Hotărîrea Guvernului nr.1021 din 16 decembrie 2013 (Monitorul Oficial al Republicii Moldova, 2013, nr.297-303, art.1129), a prevederilor Legii nr. 231 din 23.09.2010 cu privire la comerţul interior, Legii nr. 153 din 01.07.2016 pentru modificarea şi completarea unor acte legislative, Legii nr. 160 din 22.07.2011 privind reglementarea prin autorizare a activităţii de întreprinzător, Legii nr. 161 din 22.07.2011 privind implementarea ghişeului unic în desfăşurarea activităţii de întreprinzător, Hotărârii Guvernului nr. 753 din 14.06.2016 pentru aprobarea Conceptului mecanismului de gestionare şi eliberare a actelor permisive şi a Planului de acţiuni privind implementarea soluţiilor de ghişeu unic, Hotărârii Guvernului nr. 550 din 13.06.2018 cu privire la aprobarea Conceptului tehnic al Sistemului informaţional automatizat de gestionare şi eliberare a actelor permisive și Hotărârii Guvernului nr. 551 din 13.06.2018 pentru aprobarea Regulamentului cu privire la modul de ţinere a Registrului actelor permisive,

HOTĂRĂŞTE:

1. Se aprobă:

a) Modificările și completările la Conceptul Tehnic al Sistemului informaţional automatizat de gestionare şi eliberare a actelor permisive aprobat prin Hotărîrea Guvernului nr. 550 din 13.06.2018 cu privire la aprobarea Conceptului tehnic al Sistemului Informațional automatizat de gestionare și eliberare a actelor permisive (în continuare – SIAGEAP), conform anexei nr.1;

b) Modelul Regulamentului de desfăşurare a activităţilor de comerţ în localitate, conform anexei nr. 2.

c) Modelul Politicii în domeniul utilizării datelor cu caracter personal, conform anexei nr. 3;

d) Modelul Regulamentului de utilizare a datelor cu caracter personal, conform anexei nr. 4.

2. Se instituie și se pune la dispoziția Autorităților administrației publice locale și centrale ghișeul unic de tip mixt și resursa informațională în domeniul comerțului, pe baza SIAGEAP.

3. Autoritățile publice emitente de acte permisive implicate în implementarea soluţiilor de ghișeu unic din domeniul comerțului, până la data intrării în vigoare a prezentei hotărâri:

a) desemnează la nivel de instituție persoane responsabile de realizarea, coordonarea și monitorizarea implementării soluției de ghișeul unic de tip mixt și resursei informaționale în domeniul comerțului în baza SIAGEAP, informînd Ministerul Economiei și Infrastructurii în acest sens;

b) desemnează persoanele care vor opera în SIAGEAP la nivel de entitate și asigură învestirea acestora cu drepturi de utilizare și chei electronice compatibile cu serviciul guvernamental de acces M-Pass;

c) formalizează contractual, în conformitate cu reglementările în vigoare, funcționalitatea de plăți electronice M-Pay;

d) întreprind măsurile ce se impun în vederea asigurării corespunderii entității cadrului legal de utilizare/operare cu date personale, utilizînd modelele actelor conform anexei nr.3 și nr.4 ;

e) asigură, după caz, realizarea măsurilor ce se impun pentru conectarea sistemelor și registrelor informaționale proprii folosite în procesul operării cu NIAC și/sau emiterii actelor permisive la platforma guvernamentală de interoperabilitate MConnect;

f) utilizează SIAGEAP în calitate de ghișeu unic în domeniul comerțului și actelor permisive.

4. Se recomandă Autorităților administrației publice locale adoptarea Regulamentului de desfășurare a activităților de comerț în localitate, conform modelului din anexa nr. 2, până la data intrării în vigoare a prezentei hotărâri.

5. Cancelaria de Stat va asigura coordonarea şi monitorizarea la nivel central și local, a implementării soluţiilor de ghișeu unic prevăzute de prezenta Hotărâre de Guvern.

6. Prezenta Hotărâre intră în vigoare după cum urmează:

a) pentru Agenția națională pentru Sănătate Publică şi Agenţia Naţională pentru Siguranţa Alimentelor, autorităţile administraţiei publice locale ale municipiilor şi oraşelor – în termen de 2 luni de la data publicării;

b) pentru autorităţile administraţiei publice locale ale comunelor şi satelor și unitatea teritorială autonomă Găgăuzia – în termen de 6 luni de la data publicării.

PRIM-MINISTRU **Pavel FILIP**

Contrasemnează:
Ministrul economiei și Infrastructurii

Nr.__. Chişinău, _____.

Anexa nr.1
la Hotărîrea Guvernului
nr.___ din _____

**Modificările şi completările la Conceptului tehnic
al Sistemului informaţional automatizat
de gestionare şi eliberare a actelor permisive aprobat prin Hotărîrea Guvernului nr. 550
din 13.06.2018**

1. **La introducere se completează cu pct. 6^1 – 6^2 cu următorul cuprins:**
   ”6^1 Sistemul informaţional automatizat de gestionare şi eliberare a actelor permisive (SIA GEAP), propus în prezentul Concept va servi şi ca platformă pentru a realiza prevederilor legale de instituire a unei resurse informaţionale în domeniul comerţului şi a ghișeului unic pentru depunerea notificării privind inițierea activității de comerț (NIAC), va contribui la facilitarea procesului de depunere a NIAC atît pentru persoane, cît şi pentru APL. Se propune ca toate APL să utilizeze un singur sistem informaţional pentru gestionarea procesului de recepționare a NIAC și a cererilor de eliberare a actelor pemisive, comunicare şi schimb de informaţii între autoritățile publice implicate în eliberarea actelor permisive, standardizarea unor procese de prelucrare a cererilor şi eliberare a NIAC. APL care în prezent gestionează procesul de eliberare a NIAC prin intermediul sistemelor informaţionale, în cazul în care vor decide păstrarea acestora, elaborează interfeţe electronice compatibile cu SIA GEAP pentru a permite depunerea cererilor în format electronic și recepționarea actelor permisive cu stocarea lor in registrul unic de acte permisive (RAP), component integral al SIA GEAP sau vor utiliza SIA GEAP ca platformă unică în acest sens.

   6^2 SIA GEAP va servi drept bază pentru ghişeul unic de gestionare NIAC şi va integra cele mai moderne instrumente de tehnologii informaţionale pentru ca antreprenorii să economisească timp, bani şi eforturi administrative la depunerea NIAC, solicitarea şi obţinerea actelor permisive aferente. SIA GEAP va servi drept punct central pentru interconectarea APL şi coordonarea activităţilor lor, astfel ca instituţiile și entitățile implicate să poată face schimb de informaţii pentru a minimiza cantitatea de informaţii livrată de deponenți/solicitanţi în vederea obţinerii actelor permisive.

   6^3 Utilizarea unui sistem informaţional unic pentru depunerea şi gestionarea NIAC, în afară de beneficiile şi funcţionalităţile menţionate mai sus, va permite stabilirea unui mecanism pentru monitorizarea performanţei autorităţilor publice locale în procesul de eliberare a NIAC şi identificarea soluţiilor de optimizare în vederea îmbunătăţirii şi facilitării gestionării NIAC.”

2. **La dispoziții generale, pct.9 se completează cu următoarele noțiuni:**
   ”depunerea NIAC – acțiuni a comerciantului (deponentului) operate prin SIA GEAP, sau pe suport de hîrtie privind inițierea activității de comerț în baza Legii nr. 231 din 23.09.2010 cu privire la comerţul interior;
   NIAC – document recepționat/emis de SIA GEAP prin care autoritatea emitentă constată unele fapte juridice şi întrunirea condiţiilor stabilite de lege, atestând învestirea solicitantului cu o serie de drepturi şi de obligaţii pentru iniţierea, desfăşurarea şi/sau încetarea activităţii de întreprinzător sau a unor acţiuni aferente şi indispensabile acestei activităţi;

deponent NIAC - persoană fizică sau juridică care depune NIAC
APL – autoritatea administrației publice locale;
administrator – persoana împuternicită de subiecţii raporturilor juridice ai SIAGEAP în vederea mentenanței funcționalităților SIAGEAP.”

3. **Pct. 10 – 12 se expun în următoarea redacție:**
”10. SIAGEAP înglobează posibilităţile funcţionale de gestionare a fluxurilor documentare, schimbul de informaţii, funcţiile de înştiinţare, depozitare a datelor şi aplicare online, necesare pentru solicitarea şi eliberarea actelor permisive, precum și pentru depunerea și gestionarea NIAC.
11. RAP este un registru public care se ţine în scopul înregistrării actelor permisive, evidenței NIAC şi pentru a asigura informarea şi obţinerea extraselor din el de către autorităţile publice, persoanele fizice şi agenţii economici din Republica Moldova.
RAP va fi parte integrantă a resurselor informaţionale de stat.
12. SIAGEAP va pune la dispoziţia solicitanţilor următoarele servicii:
În domeniul actelor permissive:
1) obţinerea actelor permisive prin intermediul portalului de servicii publice al Guvernului;
2) asigurarea accesului la toate informaţiile necesare pentru obţinerea actelor permisive;
3) depunerea online a cererii pentru obţinerea actelor permisive;
4) depunerea online a cererii pentru obţinerea documentelor necesare pentru actele permisive;
5) achitarea online a taxelor pentru obţinerea actelor permisive;
6) schimbul electronic de informaţii legate de actele permisive între autorităţi şi sistemele lor TI;
7) semnarea electronică a documentelor.
În domeniul NIAC:
1) depunerea NIAC on-line prin intermediul portalului de servicii publice al Guvernului;
2) asigurarea accesului la toate informaţiile necesare pentru depunerea NIAC;
3) depunerea on-line a cererii pentru obţinerea actelor permisive lipsă;
4) depunerea on-line a cererii pentru obţinerea documentelor necesare pentru actele permisive;
5) achitarea online a taxelor pentru depunerea NIAC și obţinerea actelor permisive;
6) schimbul electronic de informaţii legate de actele permisive între autorităţi şi sistemele lor TI;
7) semnarea electronică a documentelor;
8) stocarea informatiilor despre acte permisive de tip NIAC emise in cadrul Registrului Unic Guvernamental de Acte Permisive (RAP).”

4. **La pct. 18 subpunctele 1) și 2) vor avea următorul cuprins:**
”1) Conturul funcţional **„ACT PERMISIV/NIAC”** include funcţii de evidenţă a:
a) NIAC și deciziilor de eliberare a actului permisiv;
b) actelor permisive emise;
c) deciziilor de refuz de eliberare a actului permisiv;
d) deciziilor de suspendare a actului permisiv;
e) notificărilor de încetare;
f) modificarea datelor din NIAC;
g) refuzul (temeiurile) de acceptare NIAC.
2) Conturul funcţional **„PARTICIPANŢI AI SISTEMULUI”** include funcţii de evidenţă a:
a) deponenților NIAC și a solicitanţilor actelor permisive;

b) APL–urilor şi autorităţilor emitente;
c) autorităţilor/entităţilor implicate în emiterea actelor permisive.
3) Conturul funcţional **„DOCUMENTE”** include funcţii de evidenţă a:
a) documentelor de intrare în SIA GEAP;
b) documentelor tehnologice ale SIA GEAP (inclusiv tehnice);
c) documentelor de ieşire ale SIA GEAP.”

5. Punctul 22 se expune în următoarea redacţie:

”Registratorii SIA GEAP sînt autoritățile administrației publice locale, conform Legii nr. 231 din 23.09.2010 cu privire la comerţul interior, autorităţile emitente de acte permisive, inclusiv autoritățile administrației publice locale, indicate în Nomenclatorul actelor permisive eliberate de către autorităţile emitente persoanelor fizice şi juridice pentru practicarea activităţii de întreprinzător (în continuare – *Nomenclator*), aprobat prin anexa nr.1 la Legea nr.160 din 22 iulie 2011 privind reglementarea prin autorizare a activităţii de întreprinzător, care introduc datele în legătură cu eliberarea actelor permisive indicate în Nomenclator și operarea cu NIAC.”

6. Punctele 24 și 25 se expun în următoarea redacţie:

”**24.** Documentele de intrare sînt următoarele:
4) cereri și NIAC;
5) rapoarte de încercări de laborator;
6) anexe la cereri;
7) documente scanate în format PDF, JPG necesare în procesul de solicitare a actului permisiv.

25. Documentele de ieşire sunt următoarele:
1) NIAC;
2) acte permisive;
3) decizie de eliberare a actului permisiv;
4) decizie de refuz de eliberare a actului permisiv;
5) rapoarte ce conţin informaţii despre actul permisiv;
6) rapoarte statistice privind NIAC și actele permisive solicitate/emise;
7) notificare (de admitere, de refuz);
8) înştiinţare de recepţionare NIAC;
9) înştiinţare privind refuzul de recepţionare NIAC;
10) notificarea de încetare NIAC;
11) notificaea de modificare a datelor din NIAC.”

7. Subpunctul 3) al pct. 27 se completează în final cu următoarele noțiuni:

”*Noțiuni aferente NIAC:*

depunerea NIAC - acțiune a deponentului NIAC prin SIA GEAP sau pe suport de hârtie conform Legii nr. 231 din 23.09.2010 cu privire la comerţul interior;

cerere – document privind solicitarea unui act permisiv care se completează de către solicitant sau AST/APL (autoritate administrației publice locale) în format electronic sau pe suport de hârtie conform scenariilor prevăzute în prezentul Concept;

înştiinţare de recepţionare a NIAC - mesaj electronic emis de către SIA GEAP pe adresa electronică specificată de solicitant, pentru confirmarea recepționarii NIAC, care urmează să conțină: – data și ora de recepţionare a notificării; – numărul de înregistrare a NIAC, acordat de APL prin intermediul SIA GEAP. Numărul unic va servi drept identificator unic a NIAC pe parcursul întregului flux de procesare; - numele şi prenumele, funcţia şi datele de contact ale persoanei responsabile din APL care a recepţionat notificarea. Înștiințarea de recepționare a NIAC recepționată în regim on-line nu acordă dreptul de începere a activității de comerț termen de 3 zile lucrătoare, în temeiul aliniatului (3) al art. 16 din Legea nr. 231/2010 privind comerțul interior;

notificare de acceptare – mesaj electronic emis de către SIA GEAP pe adresa electronică specificată de solicitant, ce conţine informaţii referitoare la acceptarea cererii privind solicitarea unui act permisiv;

înştiinţare/notificare de refuz – mesaj emis de către SIA GEAP ce conţine informaţii referitoare la refuzul de recepţionare a NIAC sau cererii privind solicitarea unui act permisiv lipsă, specificând motivul refuzului;

notificare privind o nouă NIAC sau cerere – mesaj emis de către SIA GEAP adresat utilizatorului autorităţii publice responsabil de prelucrarea datelor şi emiterea actului permisiv, ce conţine informaţii privind înregistrarea unei noi cereri;

notificare privind statutul NIAC/cererii – mesaj emis de către SIA GEAP adresat solicitantului, ce conţine informaţii privind statutul cererii pe care a depus-o;

NIAC/act permisiv emis – document electronic sau imprimat conform unui model prestabilit, după caz, recepţionat/emis de SIA GEAP prin care autoritatea emitentă constată unele fapte juridice şi întrunirea condiţiilor stabilite de lege, atestând învestirea solicitantului cu o serie de drepturi şi de obligaţii pentru iniţierea, desfăşurarea sau încetarea activităţii de întreprinzător sau a unor acţiuni aferente şi indispensabile acestei activităţi, după caz;

notificarea de încetare NIAC - acțiune a deponentului NIAC, prin intermediul SIA GEAP, prin care se notifică încetarea activității de comerț în baza unei NIAC conform Legii nr. 231 din 23.09.2010 cu privire la comerţul interior sau acțiune a operatorului în baza cererii scrise a deponentului/solicitantului;

notificarea de modificare a datelor din NIAC - acțiune a deponentului NIAC, prin intermediul SIA GEAP, prin care se notifică modificarea datelor unei NIAC conform Legii nr. 231 din 23.09.2010 cu privire la comerţul interior sau acțiune a operatorului în baza cererii scrise a deponentului/solicitantului.”

8. Subpunctul 3) al pct. 28 se completează în final cu următoarele:

” identificator al obiectului informaţional **„**NIAC**”** este codul unic de identificare, generat şi atribuit de SIAGEAP, care are următoarea structură:

„P00001/2018”, unde:

P – (tip permit);

00001 – număr;

2018 – anul emiterii;”

9. **Subpunctul 1) al pct. 29 se completează cu următoarele subpuncte**:

”14) *depunerea NIAC/cererilor prin intermediul portalului serviciilor publice (on-line)*

Prezentul scenariu este utilizat de către deponenți/solicitanţii care au acces la Internet şi se pot autentifica pe portal prin sistemul MPass/MSign utilizînd semnătura digitală. Deponenții sunt scutiţi de vizitarea autorităţilor publice responsabile de eliberarea actelor permisive şi pot să prezinte NIAC/cererea în format electronic cu anexarea documentelor necesare, de asemenea, în format electronic.

Depunerea NIAC implică următorii paşi:

a) accesarea portalului serviciilor publice: www.servicii.gov.md;

b) autentificarea în SIA GEAP prin intermediul MPass/MSign, folosind certificatul electronic;

c) parcurgerea listei de APL-uri, și acte permisive după caz, şi selectarea APL necesar;

d) completarea formularului electronic cu informaţiile necesare. Formularul va conține, de asemenea, lista de documente care urmează a fi anexate la cerere prin ataşare, după caz. În cazul notificării pentru încetarea sau modificarea NIAC, solicitantul selectează opţiunea din dosarul aferent NIAC şi indică informaţiile necesare;

e) anexarea documentelor necesare, după caz;

f) în cazul în care deponentul nu dispune de unele acte (acte permisive, alte acte sau documente) necesare pentru anexare la NIAC, acesta va depune cererea pentru obţinerea acestora

prin intermediul SIA GEAP, în cazul în care aceste funcționalități sunt disponibile (etapele pentru solicitarea actelor lipsă sunt descrise în continuare);

g) achitarea taxei pentru obținerea actelor permisive cu ajutorul Serviciului Guvernamental de Plăți Electronice (MPay), prin transfer bancar sau depunere de numerar. După efectuarea plăţii, SIA GEAP va primi confirmarea de plată prin MPay sau, în caz contrar, specialistul responsabil din cadrul autorităţii emitente va verifica faptul efectuării plăţii prin alte mijloace (cum ar fi verificarea contului bancar sau ordinului de încasare a numerarului);

h) după ce toate documentele necesare vor fi ataşate şi formularul completat, deponentul/solicitantul va putea salva NIAC/cererea cu statut de „proiect" sau o va putea semna electronic şi trimite spre examinare autorităţii publice (locale sau centrale) responsabile;

i) SIA GEAP va genera un număr unic de înregistrare al NIAC. Numărul unic va servi drept identificator unic pe parcursul întregului flux de procesare a NIAC;

j) APL/autoritatea publică emitentă de acte permisive responsabilă va primi notificarea cu privire la NIAC/cererea nouă intrată în sistem prin SIA GEAP și/sau e-mail după caz;

k) în cazul solicitării de acte permisive aferente eliberării NIAC, SIA GEAP va genera certificatul constatator privind confirmarea depunerii cererii;

l) În termen de 3 zile lucrătoare din data recepționării NIAC, APL are dreptul să emită prin SIAGEAP refuzul de recepționare a NIAC în temeiul aliniatului (3) al art. 16 din Legea nr. 231/2010 privind comerțul interior.

15) *depunerea NIAC/cererilor la sediul autorităţii publice locale (off-line)*

Prezentul scenariu va fi utilizat atunci cînd deponenții/solicitanţii vor vizita autorităţile publice locale pentru depunerea NIAC şi a cererilor de solicitarea a actelor permisive aferente NIAC, după caz. Acest scenariu implică depunerea NIAC în format de hîrtie la ghișeul APL, și procesarea acesteia și a cererilor de solicitarea a actelor permisive aferente NIAC, după caz, de către operatorii din cadrul APL prin SIA GEAP în vederea standardizării procedurii de solicitare, procesare, facilitare a schimbului de date între autorităţi şi pentru asigurarea transparenţei întregului proces de solicitare şi eliberare a actelor permisive.

Scenariul de depunere NIAC la sediul APL și solicitarea obținerii actelor permisive la sediul autorităţilor publice locale, după caz, implică următoarele etape:

a) solicitantul vizitează sediul APL;

b) reprezentantul APL oferă asistenţă deponentului la completarea corectă a NIAC pe suport de hîrtie;

c) după completare și imprimare, deponentul semnează olograf formularul NIAC, în situațiile în care sunt respectate toate cerințele legale utilizatorul APL semnează electronic NIAC iar SIA GEAP generează un număr unic de evidență și înștiințarea de recepționare (în cazul depunerii solicitării pentru încetarea sau modificarea NIAC, solicitantul depune o cerere în formă liberă cu semnătura olografă, în care se conține informația relevantă, urmată de operarea utilizatorului din cadrul APL în SIA GEAP a modificărilor necesare);

d) deponentul/solicitantul prezintă actele necesare NIAC pe suport de hîrtie în original sau copiile de pe acestea, sau pe un purtător electronic de date, originalele pot fi scanate de către utilizatorul APL, în cazul păstrării actelor anexate pe suport de hîrtie la APL în SIA GEAP se va face o mențiune în acest sens. Actele, sau informațiile (datele) privind actele care pot fi obținute prin intermediul SIA GEAP nu vor fi solicitate;

e) reprezentantul APL se autentifică în SIA GEAP prin intermediul MPass (semnăturii electronice) la orice etapă necesară;

f) reprezentantul APL completează NIAC şi cererea de eliberare a actului permisiv lipsă după caz, anexează documentele scanate sau indică datele de identificare a actelor în SIA GEAP şi semnează NIAC și/sau cererea de eliberare a actelor permisive lipsă, după caz, folosind semnătura sa electronică. NIAC sau cererea se semnează electronic de către specialistul APL pentru a autentifica că versiunea electronică a NIAC, a cererii şi a documentelor scanate sau obținute întru-un alt mod corespund documentelor depuse şi semnate de deponent/solicitant. Temei pentru depunerea cererilor de către APL către autoritățile emitente de acte permisive

lipsă, din numele deponentului/solicitantului va servi acordul în scris al deponentului/solicitantului consfinţit prin înscrierea sintagmei ”*acte permisive necesare*” în rubrica Anexe din NIAC cu semnarea olografă sub aceasta;

g) în cazul în care solicitantul semnează olograf NIAC dar nu anexează actele permisive obligatorii desfăşurării activităţii de comerţ din NIAC şi nu solicită completarea cererii de eliberare a actului permisiv lipsă, reprezentantul autorităţii publice semnează electronic NIAC iar SIA GEAP va genera un număr unic pentru NIAC cu remiterea NIAC autorităților emitente de acte permisive lipsă pentru respectarea termenului menționat la aliniatul (2) din art. 14 la Legea nr. 231/2010 cu privire la comerțul interior;

h) după completarea NIAC sau a cererii, SIA GEAP va genera factura de plată pentru achitarea taxei pentru NIAC sau actele permisive, după caz;

i) reprezentantul APL va înmîna factura de plată deponentului/solicitantului;

j) deponentul/solicitantul va achita factura la sediul băncii, la terminalele de încasare instalate în locuri publice, la subdiviziunile teritoriale ale ASP, prin Serviciul Guvernamental de Plăţi Electronice (MPay), prin transfer bancar sau în numerar;

k) după efectuarea plăţii SIA GEAP va primi confirmarea plăţii care va fi accesibilă pentru specialistul autorităţii emitente de acte permisive sau ultimul va verifica ordinul de încasare;

l) NIAC va putea să fie salvată cu statut de „proiect”, în cazul în care nu este finalizată prin semnătura olografă al deponentului, şi va fi transmisă mai tîrziu, caz în care SIA GEAP nu va genera număr de înregistrare;

m) în cazul în care cererea de eliberare a actelor permisive lipsă este completă, reprezentantul APL va remite aceasta prin intermediul SIA GEAP la autoritatea publică responsabilă de eliberare a actului permisiv;

n) SIA GEAP va genera un număr unic de înregistrare al NIAC şi al cererii de eliberare a actului permisiv lipsă după caz, la introducerea acesteia în sistem de către utilizatorul din cadrul APL. Numărul unic al NIAC şi cererii după caz, va fi folosit de către APL pentru a monitoriza statutul NIAC şi al cererii prin SIA GEAP;

o) autoritatea publică emitentă implicată va primi, prin SIA GEAP și/sau prin e-mail, NIAC și/sau cererea nouă intrată în sistem;

16) *scenariul pentru obţinerea documentelor lipsă la NIAC constă din următoarele etape:*

a) utilizatorul din cadrul cadrul APL completează cererea de obţinere a actului permisiv lipsă iar solicitantul semnează cererea pe hîrtie;

b) formularul de cerere deschide lista documentelor care trebuie să fie anexate la cerere;

c) pentru fiecare act care urmează să fie anexat, utilizatorul poate ataşa actul electronic (scanat) sau poate să solicite documentul prin apăsarea butonului „Solicită”, funcţie disponibilă pentru fiecare document din listă;

d) după apăsarea butonului „Solicită”, se deschide noul formular de cerere şi utilizatorul completează cererea pentru obţinerea documentului necesar. Procesul de completare a cererii şi de achitare a taxei pentru obţinerea documentului este similar cu procesul standard de depunere a cererilor primare descrise în scenariile generale ale SIA GEAP pentru actele permisive, deponentul/solicitant urmând să prezinte proba achitării serviciului, în cazul în care acest serviciu este taxat;

e) în cazul în care nu sînt ataşate toate documentele, cererea este salvată cu statut de „proiect”, iar solicitantul/utilizatorul din cadrul APL poate continua completarea cererii mai tîrziu, cînd va obţine toate documentele necesare completării cererii;

f) după obţinerea documentelor necesare, solicitantul/ utilizatorul din cadrul APL accesează cabinetul personal şi deschide proiectul cererii;

g) anexează documentele necesare obținute pentru obținerea NIAC sau altui act permisiv după caz;

17) *analiza şi procesarea cererii de către autoritatea publică responsabilă de eliberarea actelor permisive în cazul NIAC:*

a) prezentului scenariu i se aplică procedura generală pentru actele permisive.

b) autoritățile publice emitente de acte permisivă vor informa APL corespondentă prin SIA GEAP privind decizia în speță.

18) *scenariul privind modificarea/suspendarea/încetarea NIAC* se declanşează de către specialistul responsabil din cadrul autorităţii emitente a actului permisiv

Prezentul scenariu constă din următoarele etape:

a) în baza autosesizării sau notificării SIA GEAP, specialistul din cadrul autorităţii emitente despre necesitatea de a accesa dosarul NIAC;

b) specialistul din cadrul autorităţii emitente a NIAC accesează dosarul NIAC în SIA GEAP şi accesează NIAC respectivă;

c) statutul actului permisiv se modifică doar după aprobarea conducerii autorităţii notificată în acest sens care decide privind modificarea statutului actului permisiv:

1) aprobă schimbarea statutului NIAC prin semnarea opțiunii respective (olografă sau digitală, în dependență de procedura stabilită)

2) refuză schimbarea statutului NIAC prin semnarea opțiunii respective (olografă sau digitală, în dependență de procedura stabilită) cu indicarea în clar a temeiurilor legale;

d) pentru *modificarea/suspendarea/încetarea* NIAC, specialistul modifică statutul actului în „Suspendat", „Activ", „Nevalabil" sau "Modificat" şi anexează documentele necesare în baza cărora (data şi numărul deciziei/actului) se efectuează *modificarea/suspendarea/încetarea* NIAC.

e) SIA GEAP notifică beneficiarul/posesorul NIAC actului permisiv despre schimbarea statutului.

19) *scenariul privind aprobarea tacită a actului permisiv în cazul NIAC:*

a) aprobarea tacită pentru actele permisive lipsă solicitate de către APL prin intemediul SIA GEAP survine pentru deponent/solicitant în baza Legii nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător și a scenariilor de mai sus aplicabile. Cetificatul constatator va fi emis pe adresele electronice ale solicitantului/deponentului și AOL corespondent".

10. Punctul 29 se completează cu un subpunct nou 11):

"11) **date privind obiectul informaţional „NIAC":**

a) ID – numărul de identificare;
b) titlu;
c) data şi timpul depunerii cererii;
d) IDNO/IDNP al solicitantului;
e) domiciliul deponentului;
f) date de contact: telefon fix; telefon mobil; fax; E-mail (obligatoriu în cazul operării on-line);
g) IDNO al APL;
h) IDNP sau datele de identificare electronice (MPass/MSign) după caz, al utilizatorului APL care a oprează NIAC;
i) statut (recepționat, proiect, semnat, trimis, executat);
j) termenul-limită de procesare a NIAC după caz;
k) alte documente necesare pentru operarea NIAC (actului permisiv, anexe, etc.);
l) ID al deciziei de acceptare sau refuz pentru NIAC/act permisiv;
m) pentru unitatea comercială/loc de vînzare (adresa, tipul (Codul CAEM), suprafața comercială (m^2);
n) pentru unităţile de alimentaţie publică (capacitatea unității comerciale (numărul de locuri/persoane), inclusiv la terasă (numărul de locuri/persoane),
o) comercializarea producţiei alcoolice, comercializarea berii, comercializarea produselor din tutun, desfăşurarea comerţului ambulant, comercializarea prin intermediul unităţii mobile, comercializarea prin aparat comercial (cu opțiunea DA/NU);
p) privind unitatea mobilă (tipul, lungimea, lățimea, înălțimea);

q) privind comercializarea prin aparat comercial (numărul de aparate, lungimea, lățimea, înălțimea);
r) Anexe (cîmp deschis, sau sintagme solicitării de acte permisive lipsă);
s) Declarația de proprie răspundere ți asumarea de obligații;"

Anexa nr.2
la Hotărîrea Guvernului
nr.___ din _____

MODELUL
Regulamentului de desfăşurare
a activităţilor de comerţ în localitate

CONSILIUL
[se indică denumirea completă a consiliului]
D E C I Z I E
Nr. [numărul deciziei] din [data deciziei]

În vederea stabilirii interdicţiilor şi cerinţelor privind desfăşurarea activităţii de comerţ în [se indică localitatea] , în temeiul art.6 alin.(1) lit.n) şi alin.(5) din Legea nr.231 din 23 septembrie 2010 cu privire la comerțul interior (Monitorul Oficial al Republicii Moldova, 2010, nr.206-209, art.681) și art.14 alin.(2) lit.q) din Legea nr.436 din 28 decembrie 2006 privind administraţia publică locală (Monitorul Oficial al Republicii Moldova, 2007, nr.32-35, art.116), CONSILIUL [se indică denumirea completă a consiliului]

DECIDE:

1. Se aprobă Regulamentul de desfăşurare a activităţii de comerţ în [se indică localitatea, conform denumirii oficiale la forma gramaticală respectivă în continuare după text] (în continuare – Regulament), conform anexei. Persoanele fizice și juridice care desfășoară activități de comerț în localitatea [se indică localitatea], sînt obligaţi să prevederile Regulamentului.
3. Se aduce la cunoștința persoanelor fizice și juridice care desfășoară activități de comerț că prevederile Regulamentului nu anulează și nu substituie prevederile Legea nr.231 din 23 septembrie 2010 cu privire la comerțul interior și altor acte normative în vigoare, ci stabilește interdicţii şi cerinţe suplimentare la desfăşurarea activităţii de comerţ în [se indică localitatea].
4. În cazul desfăşurării activităţii de comerţ cu încălcarea prevederilor legislaţiei şi/sau Regulamentui, persoana fizică şi persoana juridică este pasibilă răspunderii contravenționale, conform Codului contravenţional, suspendării și/sau încetării activității de comerţ.
5. Se recomandă persoanelor fizice și juridice care desfășoară activități de comerț în [se indică localitatea] examinarea și studierea Ghidului privind desfășurarea activității de comerț, amplasat pe pagina web www.mec.gov.md.

6. Persoanele fizice și juridice sînt în drept să înainteze propuneri de modificare și completare a Regulamentului, cu expedierea acestora în adresa autorităților administrației publice locale din [se indică localitatea] .
7. Controlul executării prezentei decizii și respectării prevederilor Regulamentului, în limitele stabilite de art.22 alin.(4) și (5) din Legea cu privire la comerțul interior, se pune în sarcina [persoana sau subdiviziunea responsabilă].
8. [persoana sau subdiviziunea responsabilă] :
a) va monitoriza modul de aplicare și implementare a prevederilor Regulamentului și va prezenta Consiliului anual un raport privind desfășurarea activităților de comerț în [se indică localitatea];
b) va înainta Consiliului, la necesitate, propuneri de modificare și completare a Regulamentului.
9. Prezenta Decizie intră în vigoare [se indică data sau modul de intrare în vigoare].

Președinte [se indică numele președintelui Consiliului sau ședinței]
Contrasemnează: [se indică numele secretarului]

Anexă unică
la Decizia Consiliului *[se indică denumirea completă a consiliului]*
nr.*[numărul deciziei]* din *[data deciziei]*

REGULAMENTUL
de desfăşurare a activităţii de comerț în
[se indică localitatea]

I. DISPOZIȚII GENERALE

Regulamentul de desfăşurare a activităţii de comerț în [se indică localitatea, conform denumirii oficiale la forma gramaticală respectivă în continuare după text] (în continuare "Regulament") este elaborat în scopul creării unui mediu favorabil de desfășurare a activității de întreprinzător în cadrul localității, precum și în vederea asigurării liberei concurențe, protecţiei vieții, sănătăţii, securității și intereselor economice și sociale ale cetățenilor.

Prezentul Regulament stabilește interdicţiile şi cerinţele de desfăşurare a activităţii de comerț în [se indică localitatea] în conformitate cu prevederile art.6 alin.(1) lit.n) şi alin.(5) din Legea nr.231 din 23 septembrie 2010 cu privire la comerțul interior, în următoarele privințe:
1) interdicţia de a desfăşura activităţi de comerț sau anumite forme ale activităţii de comerț, inclusiv comerțul ambulant, în perimetrul anumitor zone sau străzi ori în intervalul anumitor zile sau ore;
2) modul de desfăşurare a activităţilor de comerț în apropierea edificiilor autorităţilor publice, instituţiilor de învăţământ, instituţiilor medicale, lăcaşurilor de cult, monumentelor, lucrărilor de artă, edificiilor cu valoare arhitecturală, istorică sau arheologică, zonelor storice,
precum şi în locurile (destinaţiile) de interes turistic;
3) distribuirea activităţilor de comerț între zona centrală şi zonele periferice ale localităţii, precum şi între zonele aglomerate şi cele neaglomerate;

4) raza în care este interzisă comercializarea producţiei alcoolice în preajma instituţiilor de învăţământ, instituţiilor medicale şi lăcaşurilor de cult;
5) cerinţe privind regimul de lucru (orarul de funcţionare) al comercianţilor în perimetrul anumitor zone sau străzi;
6) interdicţia de a comercializa anumite produse sau servicii în perimetrul anumitor zone sau străzi.

Noțiunile din prezentul Regulament au semnificația stabilită de Legea nr.231 din 23 septembrie 2010 cu privire la comerțul interior și alte acte normative în vigoare.

II. INTERDICŢIA DE DESFĂŞURARE A ACTIVITĂŢI DE COMERŢ

Se interzice desfăşurarea activităţi de comerţ în perimetrul următoarelor străzi și zone:
1) [se indică perimetrul străzilor sau zonelor] ;
2) [se indică perimetrul străzilor sau zonelor] ;
3) [se indică perimetrul străzilor sau zonelor] .

III. INTERDICŢII PRIVIND DESFĂȘURAREA UNOR FORME DE COMERȚ

Secțiunea 1. Comerţul ambulant

Se permite/interzice desfășurarea comerțului ambulant în perimetrul următoarelor străzi și zone:
1) [se indică perimetrul străzilor sau zonelor] ;
2) [se indică perimetrul străzilor sau zonelor] ;
3) [se indică perimetrul străzilor sau zonelor] .

Străzile și zonele în perimetrul cărora este permisă/interzisă desfășurarea comerțului ambulant sînt marcate cu roșu în Anexa nr. 2 la Regulament.

Secțiunea 2. Activitatea piețelor

Se permite/interzice desfășurarea activității piețelor în perimetrul următoarelor străzi și zone:
1) [se indică perimetrul străzilor sau zonelor] ;
2) [se indică perimetrul străzilor sau zonelor] ;
3) [se indică perimetrul străzilor sau zonelor] .

Străzile și zonele în perimetrul cărora este permisă/interzisă activitatea piețelor sînt marcate
cu roșu în Anexa nr.3 la Regulament.

IV. DESFĂŞURAREA ACTIVITĂŢII DE COMERŢ ÎN APROPIEREA EDIFICIILOR ŞI ZONELOR STABILITE DE LEGE

Secțiunea 1. Activitatea de comerţ în apropierea unor edificii

Activitatea de comerţ în perimetrul a [se indică perimetrul (distanța în metri de la edificii)] de la edificiile autorităţilor publice, instituţiilor de învăţământ, instituţiilor medicale, lăcaşurilor de cult, monumentelor, lucrărilor de artă, edificiilor cu valoare arhitecturală, istorică sau arheologică, conform listei stabilite de Anexa nr.4, se desfășoară cu respectarea următoarelor cerințe:
1) [se indică cerința care trebuie respectată de comerciant] ;
2) [se indică cerința care trebuie respectată de comerciant] ;
3) [se indică cerința care trebuie respectată de comerciant] .

Secțiunea 2. Activitatea de comerţ în anumite zone

Activitatea de comerţ în zonele istorice şi în locurile (destinaţiile) de interes turistic, stabilite de Anexa nr.5, se desfăşoară cu respectarea următoarelor cerinţe:
1) [se indică cerința care trebuie respectată de comerciant] ;
2) [se indică cerința care trebuie respectată de comerciant] ;
3) [se indică cerința care trebuie respectată de comerciant] .

V. INTERDICŢII PRIVIND COMERCIALIZA UNOR PRODUSE SAU PRESTAREA UNOR SERVICII

Secțiunea 1. Comercializarea producţiei alcoolice

Se interzice comercializarea producției alcoolice în raza a [se indică raza stabilită de APL]
din preajma instituţiilor de învăţământ, instituţiilor medicale şi lăcaşurilor de cult, indicate în Anexa nr.4 la prezentul Regulament.

Secțiunea 2. Jocuri de noroc

Se permite/interzice amplasarea sălilor de joc şi aparatelor de joc, și desfășurarea jocurilor de noroc, în condițiile stabilite de pct.__, doar în perimetrul următoarelor străzi şi zone:
1) [se indică perimetrul străzilor sau zonelor] ;
2) [se indică perimetrul străzilor sau zonelor] ;
3) [se indică perimetrul străzilor sau zonelor] .

Desfășurarea jocurilor de noroc se permite doar în intervalul următoarelor ore/zile [se indică zilele/orele pe parcursul cărora activitatea în cauză este permisă] .

Străzile și zonele în perimetrul cărora este permisă/interzisă amplasarea sălilor de joc și aparatelor de joc, și desfășurarea jocurilor de noroc sînt marcate cu roșu în Anexa nr.6 la Regulament.

Secțiunea 3. Interdicții privind desfășurarea [se indică activitatea de comerț interzisă]

Se interzice desfășurarea [se indică activitatea de comerț interzisă] în perimetrul următoarelor străzi și zone:
1) [se indică perimetrul străzilor sau zonelor] ;
2) [se indică perimetrul străzilor sau zonelor] ;
3) [se indică perimetrul străzilor sau zonelor] .

Străzile și zonele în perimetrul cărora este interzisă desfășurarea activității de comerț stabilită de pct.__ sînt marcate cu roșu în Anexa nr.7 la Regulament.

Interdicția stabilită de pct.__ se aplică doar în intervalul orelor/zilelor [se indică zilele/orele pe parcursul cărora activitatea în cauză este interzisă] .

Secțiunea 4. Interdicții privind comercializarea [se indică bunurile comercializarea
cărora este supusă restricțiilor]

Se interzice comercializarea [se indică bunul, comercializarea căruia este supusă restricțiilor] în perimetrul următoarelor străzi și zone:
1) [se indică perimetrul străzilor sau zonelor] ;
2) [se indică perimetrul străzilor sau zonelor] ;
3) [se indică perimetrul străzilor sau zonelor] .

Străzile și zonele în perimetrul cărora este interzisă comercializarea bunului stabilit de pct.__ sînt marcate cu roșu în Anexa nr.8 la Regulament.

Interdicția stabilită de pct.0 se aplică doar în intervalul orelor/zilelor [se indică zilele/orele pe parcursul cărora activitatea în cauză este interzisă].

VI. CERINȚE PRIVIND REGIMUL DE LUCRU AL COMERCIANŢILOR

Se interzice desfășurarea activității de comerț în intervalul orelor/zilelor [se indică zilele/orele pe parcursul cărora activitatea în cauză este interzisă] în perimetrul următoarelor străzi și zone:
1) [se indică perimetrul străzilor sau zonelor] ;
2) [se indică perimetrul străzilor sau zonelor] ;
3) [se indică perimetrul străzilor sau zonelor] .

Străzile și zonele în perimetrul cărora desfășurarea activității de comerț este interzisă în intervalul orelor/zilelor conform pct.0 sînt marcate cu roșu în Anexa nr.4 la Regulament.

Anexa nr.1 la Regulamentul de desfăşurare a activităţii de comerț în [se indică localitatea]
Străzile și zonele în perimetrul cărora este interzisă desfășurarea activității de comerț (MODEL)

Anexa nr.2 la Regulamentul de desfăşurare a activităţii de comerț în [se indică localitatea]

Străzile și zonele în perimetrul cărora este permisă desfășurarea comerțului ambulant (MODEL extras de pe hartă)

Anexa nr.3 la Regulamentul de desfăşurare a activităţii de comerț în [se indică localitatea]

Străzile și zonele în perimetrul cărora este permisă activitatea piețelor (MODEL și/sau extras de pe hartă)

Anexa nr.4 la Regulamentul de desfăşurare a activităţii de comerț în [se indică localitatea]

Lista edificiilor autorităţilor publice, instituţiilor de învăţământ, instituţiilor medicale, lăcaşurilor de cult, monumentelor, lucrărilor de artă, edificiilor cu valoare arhitecturală, istorică sau arheologică din [se indică localitatea] (MODEL)

Autorităţi publice	**Adresa**
Guvernul Republicii Moldova	Piaţa Marii Adunări Naţionale, 1
Ministerul Afacerilor Interne	Bd. Ştefan cel Mare şi Sfint, nr. 75

Anexa nr.5 la Regulamentul de desfăşurare a activităţii de comerț în [se indică localitatea]

Zonele istorice şi locurile (destinaţiile) de interes turistic din [se indică localitatea, și/sau extras de pe hartă] (MODEL)

Anexa nr.6 la Regulamentul de desfăşurare a activităţii de comerț în [se indică localitatea]

Străzile și zonele în perimetrul cărora este interzisă amplasarea sălilor de joc și aparatelor de joc, și desfășurarea jocurilor de noroc

Anexa nr.7 la Regulamentul de desfăşurare a activităţii de comerț în [se indică localitatea]

Străzile și zonele în perimetrul cărora este interzisă desfășurarea [se indică activitatea de comerț interzisă]

Anexa nr.8 la Regulamentul de desfăşurare a activităţii de comerţ în [se indică localitatea]

Străzile şi zonele în perimetrul cărora este interzisă comercializarea [se indică bunul, comercializarea căruia este supusă restricţiilor]

Anexa nr.9 la Regulamentul de desfăşurare a activităţii de comerţ în [se indică localitatea]

Străzile şi zonele în perimetrul cărora desfăşurarea activităţii de comerţ este interzisă în intervalul anumitor ore/zilele.

Anexa nr.3
la Hotărîrea Guvernului
nr.___ din _____

Modelul
Politicii în domeniul utilizării datelor cu caracter personal

CONSILIUL
[se indică denumirea completă a consiliului]

D E C I Z I E
Nr. [numărul deciziei] din [data deciziei]

Cu privire la aprobarea Politicii de securitate
a datelor cu caracter personal în [se indică localitatea, conform denumirii oficiale la forma gramaticală respectivă în continuare după text]

În temeiul prevederilor art.30 alin.(l) şi alin.(3) al Legii nr.l 33 din 08.07.2011 privind protecţia datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2011, nr.170-175, art.492), şi apct.17-19 din Hotărîrea Guvernului nr.1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (Monitorul Oficial al Republicii Moldova, 2010, nr.254-256, art.1282),

DECIDE:

1. Se aprobă Politica de securitate a datelor cu caracter personal în cadrul [se indică localitatea] conform anexei.
2. Se desemnează [se indică persoana], [se indică funcţia], în calitate de persoană responsabilă de implementarea şi monitorizarea Politicii de securitate a datelor cu caracter personal, precum şi de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei care conţine date cu caracter personal.
3. Angajaţii Primăriei [se indică localitatea] implicaţi în prelucrarea datelor cu caracter personal, poartă răspundere personală pentru respectarea Politicii de securitate a datelor cu caracter personal.
4. Controlul privind executarea prezentului ordin se pune în sarcina dlui [se indică persoana şi funcţia].

Preşedinte [se indică numele preşedintelui Consiliului sau şedinţei]

Contrasemnează: [se indică numele secretarului]

Anexă unică
la Decizia Consiliului [se indică denumirea completă a consiliului]
nr.[numărul deciziei] din [data deciziei]

POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL
ÎN CADRUL [se indică localitatea]

I. Introducere

1. Politica de securitate a datelor cu caracter personal este aprobată de către Consiliul [se indică localitatea, conform denumirii oficiale la forma gramaticală respectivă în continuare după text], care acţionează în baza [se indică actul normativ] şi are sediul înregistrat pe adresa: [se indică adresa completă].
2. Politica este aprobată, în vederea conformării Consiliul [se indică localitatea] cu prevederile Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal şi cu prevederile Hotărîrii Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.
3. La prelucrarea datelor cu caracter personal în cadrul entităţii sunt aplicate principiile prevăzute de actele internaţionale: Declaraţia universală a drepturilor omului, Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale, Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Directiva 95/46/CE a Parlamentului European şi a Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, şi a celor naţionale: Constituţia Republicii Moldova, Legea nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal, Legea nr.982 din 11.05.2000 privind accesul la informaţie, Hotărîrea Guvernului nr.1123 din 14 decembrie 2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin, Hotărîrea Guvernului nr.296 din 15 mai 2012 privind aprobarea Regulamentului Registrului de evidenţă al operatorilor de date cu caracter personal, precum şi alte acte normative de profil.

II. Noţiuni generale

4. In prezenta Politică de securitate, sînt definite/utilizate următoarele noţiuni:

date cu caracter personal - orice informaţie referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

categorii speciale de date cu caracter personal - datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenenţa socială, datele privind starea de sănătate sau viaţa sexuală, precum şi cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancţiunile contravenţionale;

operator - persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituţie ori organizaţie care, în mod individual sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislaţia în vigoare;

persoană împuternicită de către operator - persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor primite de la operator;

autentificare - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

control de securitate - acţiuni întreprinse de către [se indică localitatea]în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute;

fişiere temporare - ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat pînă la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare - atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

integritate - certitudinea, necontradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;

mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal - mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;

nivel de protecţie - nivel de securitate proporţional riscului pe care îl comportă prelucrarea faţă de datele cu caracter personal respective, precum şi faţă de drepturile şi libertăţile persoanelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri;

politica de securitate a datelor cu caracter personal - document, elaborat de către operatorul de date - [se indică localitatea], care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinîndu-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile la care sînt expuse acestea;

perimetru de securitate - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic şi/sau tehnic al accesului;

persoana responsabilă de politica de securitate a datelor cu caracter personal - persoana responsabilă de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei care conţine date cu caracter personal, precum şi de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a deţinătorului de date cu caracter personal;

protecţia informaţiei contra acţiunilor neintenţionate - ansamblu de măsuri a acţiunilor neintenţionate, provocate de erorile utilizatorului, inico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;

purtător de date cu caracter personal - suport magnetic, optic, laser, de hîrtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia;

restaurarea datelor - procedurile cu privire la reconstituirea/prestabilirea datelor cu caracter personal în sxarea în care se aflau pînă la momentul pierderii sau distrugerii acestora;

tehnologie informaţională - totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

utilizator - perse ana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;

sesiune de lucru - perioada care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale şi pînă la momentul opririi acestora;

sistem informaţional de date cu caracter personal - totalitatea resurselor şi tehnologiilor informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie care conţine date cu caracter personal;

prelucrarea datelor cu caracter personal - orice operaţiune sau serie de operaţiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautiomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;

stocare - păstrarea pe orice fel de suport a datelor cu caracter personal;

sistem de evidenţă a datelor cu caracter personal - orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentraizată ori repartizată după criterii funcţionale sau geografice;

consimţământul subiectului datelor cu caracter personal - orice manifestare de voinţă liberă, expresă şi necondiţionată, în formă scrisă sau electronică, conform cerinţelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;

depersonalizarea datelor - modificarea datelor cu caracter personal astfel încît detaliile privind circumstanţele personale sau materiale să nu mai permită atribuirea acestora unei persoane doar în condiţiile unei fizice identificate sau identificabile ori să permită atribuirea investigaţii care necesită cheltuieli disproporţionate de timp, mijloace şi forţă de muncă.

III. Obiectivele Politicii de securitate a datelor cu caracter personal

5. Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv a datelor cu caracter personal prelucrate de [se indică localitatea], atît în cadrul prelucrării manuale, cît şi în cadrul sistemelor şi proceselor de tehnologie informaţională.

6. Securitatea rejrezintă o componentă esenţială a derulării optime a proceselor bazate pe TI în cadrul [se indică localitatea]. Baza unei securităţi TI adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv a datelor cu caracter personal, a sistemelor şi proceselor TI împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislaţiei.

7. Avînd în vedere că siguranţa TI nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic şi de altă natură.

8. [se indică localitatea] va proteja datele cu caracter personal atît a participanţilor la proces/vizitatori, cît şi a angajaţilor săi.

9. Reglementările prezentei Politici reprezintă un standard minim pentru [se indică localitatea], inclusiv toţi angajaţii [se indică localitatea], care vor respecta strict prevederile Politicii şi a regulilor interne privind protecţia datelor cu caracter personal şi sistemelor TI.

IV. Scopul aplicării măsurilor de protecţie a datelor cu caracter personal

10. Măsurile de protecţie a datelor cu caracter personal sunt asigurate în scopul:

1) preîntîmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

2) preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;
3) neadmiterea dezvăluirii terţilor a informaţiei cu accesibilitate limitată;
4) eficientizarea resurselor informaţionale atît pe suport de hîrtie cît şi cel în format electronic.

V. Metodele de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale

11. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:
1) preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
2) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
3) preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
4) preîntîmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor precum şi a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
5) preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea canalelor VPN;
6) preîntîmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă;
7) scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent;
8) stabilirea exactă a ordinii de acces la informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenţă instituite atît cît şi pentru cei externi.

VI. Resursele informaţionale supuse principiilor de protecţie a datelor cu caracter personal

12. Protecţia datelor cu caracter personal în cadrul [se indică localitatea] (în calitate de operator de date cu caracter personal) este asigurată printr- un complex de măsuri tehnice şi organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal.
13. Sînt supuse protecţiei prin mijloace/procedee specifice, toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin date cu caracter personal, păstrate pe:
1) suporturi magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive infonnaţionale şi baze de date;
2) sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv are şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei.

VII. Dispoziţii privind ierarhia şi obligaţiile persoanei responsabile de Politica de securitate a datelor cu caracter personal

14. Operatorul de date cu caracter personal reieşind din specificul activităţii, prin prezenta Politică de securitate, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecţie la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidenţă gestionate.
15. Politica de securitate a datelor cu caracter personal se va revizui cel puţin o dată în an ca rezultat al modificărilor sau reevaluării competenţelor entităţii, fiind pusă în sarcina conducătorilor, de a desemna persoana/ele care vor purcede nemijlocit la ajustarea prevederilor prezentului act.
16. Politica de securitate, în mod obligatoriu va fi adusă la cunoştinţă, sub semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.
17. Responsabil de implementarea şi monitorizarea respectării prevederilor datelor cu caracter personal, va fi desemnată persoana care conform fişei postului şi/sau ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.
18. Persoana responsabilă desemnată, indiferent de funcţiile exercitate, în cadrul monitorizării implementării/respectării prevederilor Politicii de securitate, se va subordona nemijlocit conducătorului [se indică localitatea] sau persoanei care îndeplineşte interimatul funcţiei.
19. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.
20. Persoana responsabilă de politica de securitate a datelor cu caracter personal întreprinde următoarele acţiuni:
1) defineşte clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală;
2) asigură măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţi datelor cu caracter personal;
3) elaborează prpcedurile de clasificare a informaţiei care conţine date cu caracter personal, astfel încît să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date;
4) instruieşte persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

VIII Procedurile organizatorice şi tehnice la prelucrarea datelor cu caracter personal

Secţiunea 1
Măsurile generale de administrare a securităţii informaţionale

21. Măsurile generale de administrare a securităţii informaţionale sunt următoarele:
1) în cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.
2) Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.

3) Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.
4) Este asigurată securitatea şi accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.
5) Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.
6) Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.
7) Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

Secţiunea 2
Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal

22. Accesul în sediile/oficiile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au permisiunea necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).
23. Se asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces.
24. Perimetrul de securitate al [se indică localitatea] reprezintă perimetrul oficiilor în care se prelucrează/stochează date cu caracter personal.
25. Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sînt rezistenţi, intrările sunt echipate cu lacăte şi semnalizare.
26. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
27. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc persoanele desemnate.
28. Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
29. Accesul în perimetrul de securitate al clădirii [se indică localitatea] unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ţinînd cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 şi art. 30 al Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal, precum şi pct. 26 din Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.
30. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii.

Secţiunea 3 Identificarea şi autentificarea utilizatorilor şi echipamentului. Administrarea identificatorilor utilizatorilor

31. Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.
32. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conţine semnalmentele nivelului de accesibilitate al utilizatorului.
33. Pentru confirmarea ID-ului utilizatorului pot fi utilizate: parole; mijloace fizice speciale de acces cu memorie (token); cartele cu microprocesoare; mijloace biometrice de autentificare bazate pe caracteristici unice şi individuale ale persoanei.
34. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile sau culpe, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă sau se suspendă de administratorul TI.
35. Administrarea identificatorilor utilizatorilor include:
1) identificarea univocă a fiecărui utilizator;
2) verificarea autenticităţii fiecărui utilizator.
36. Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal, cu menţinerea acestor informaţii pentru o perioadă îndelungată.

Secţiunea 4
Utilizarea parolelor în procesul asigurării securităţii informaţionale. Controlul administrării accesului

37. La utilizarea parolelor sunt respectate regulile de asigurare a securităţii informaţionale care prevăd:
1) păstrarea confidenţialităţii parolelor;
2) interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;
3) modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei;
4) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere;
5) modificarea parolelor peste intervale de 3 luni;
6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).
38. Controlul sistematic al acţiunilor utilizatorilor se efectuează în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Secţiunea 5
Accesul de la distanţă Limitarea folosirii tehnologiilor fără fir

39. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate, supuse monitorizării şi controlului.
40. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este permisă de persoanele responsabile din cadrul [se indică localitatea] şi permisă doar utilizatorilor, cărora aceasta le este necesară pentru îndeplinirea obiectivelor stabilite,

41. Accesul fară fir la sistemele informaţionale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării şi controlului.
42. Accesul fară fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.
43. Folosirea tehnologiilor fară fir se permisă de persoanele responsabile din cadrul [se indică localitatea].

Secţiunea 6
Securitatea electroenergetică.
Controlul instalării şi scoaterii componentelor TI

44. Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.
45. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.
46. Sunt implementate sisteme automatizate de depistare şi semnalizare a incendiilor în birourile unde sînt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.
47. Este exercitat controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal.
48. Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţie, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.

Secţiunea 7
Dezvăluirea datelor cu caracter personal

49. Dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informaţii sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN.
50. Accesul fară fir la sistemele de evidenţă a datelor cu caracter personal este permis doar utilizatorilor autorizaţi. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieşind din posibilităţile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi.
51. În cazul în care reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmînarea personală, etc.).
52. Este interzisă dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund Cerinţelor (spre exemplu: expedierea informaţiei prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.). O astfel de desiminare este posibilă urmare a indicării de către deponent/solicitant a adresei electronice în depunere/solicitare/cerere.
53. Sunt interzise operaţiunile de dezvăluire a datelor cu caracter personal între [se indică localitatea] şi alte entităţi care sunt amplasate geografic în stînga Nistrului (regiunea transnistreană) care refuză să se supună juridic legislaţiei Republicii Moldova, reieşind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei

părţi teritoriale, inclusiv în partea ce ţine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal.

54. Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie şi/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituţional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecţie a datelor cu caracter personal.

55. Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art.32 al Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal, în special în cazurile cînd tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

56. Volumul şi categoriile datelor cu caracter personal colectate în scopul ţinerii evidenţei activităților [se indică localitatea], este limitat la strictul necesar pentru realizarea scopurilor declarate.

57. Acces la sistemele informaţionale gestionate în cadrul [se indică localitatea], din partea Procuraturii Generale (după caz procuraturile teritoriale/specializate), Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art.15 şi art.212 al Codului de procedură penală.

Se explică că, în conformitate cu prevederile art.157 al Codului de procedură penală, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adeverite circumstanţe care au importanţă pentru cauză (inclusiv informaţia stocată în auditul sistemelor informaţionale şi de evidenţă), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 al Codului de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate şi răspîndite fară necesitate informaţie oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată (inclusiv operatorii de date cu caracter personal) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informaţii o explicaţie în scris care ar confirma necesitatea furnizării datelor menţionate.

Urmează a se lua act de faptul că, în conformitate cu prevederile art.8 al Legii nr.982 din 11.05.2000 privind accesul la informaţie, datele cu caracter personal fac parte din categoria informaţiei oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislaţiei privind protecţia datelor cu caracter personal.

58. În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoştinţă cu fişa personală a clientului, aceştia urmează a fi informaţi în scris despre obligaţiile ce le revin în conformitate cu prevederile art.15 al Codului de procedură penală, art. 29 şi art.30 al Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art.741 al Codului Contravenţional.

Secțiunea 8
Drepturile subiecțiiler de date cu caracter personal

59. În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal, acestuia i se furnizează următoarele informaţii, exceptînd cazul în care subiectul deţine deja informaţiile respective:

1) privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea. adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidenţă al operatorilor de date cu caracter personal);
2) privind scopul concret al prelucrării datelor cu caracter personal colectate;
3) privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
4) dreptul la informare şi de acces la datele colectate, de intervenţie asupra datelor (în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia;
5) dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine.

60. Persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţi subiecţi, conţinute în fişele personale (alte materiale), cu excepţia cazurilor în care solicitanţii îşi realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

61. Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entităfile ce asigură mentenaţa sistemului şi sau prestează servicii externalizate ale operatorului) tuturor persoanelor supuse prelucrării.

62. În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenţie, datele inexacte vor fi actualizate prin rectificare sau ştergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaţionale principale de stat etc.), modificarea urmînd a fi efectuată în toate sistemele informaţionale şi de evidenţă gestionate.

Secţiunea 9
Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate

63. Accesul în spaţiile/perimetrul unde sînt amplasate sistemele informaţionale şi de evidenţă a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au permisiunea necesară conform politicii de securitate instituţionale /regulamentelor departamentale aprobate.

64. Este interzisă stocarea şi păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecţie speciale tehnice şi de program şi nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii softului, de asigurare a efectuării periodice a copiilor de siguranţă şi de efectuare a auditului.

65. Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă.

66. Accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredinţate doar persoanei responsabile desemnate pentru implementarea Politicii de securitate din cadrul [se indică localitatea].

67. Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie.

68. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

Secţiunea 10
Auditul sistemelor informaţionale gestionate

69. Înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem se efectuează conform următorilor parametri:
a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.
70. Înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, se efectuează conform următorilor parametri:
a) data şi timpul tentativei de obţinere a accesului (executate a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau procesului, sau ID-ul utilizatorului;
c) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
d) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
e) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.
71. Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:
a) data şi timpul modificării competenţelor;
b) ID-ul administratorului care a efectuat modificările;
c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.
72. Înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces se efectuează conform următorilor parametri:
a) data şi timpul eliberării;
b) denumirea informaţiei şi căile de acces la aceasta;
c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
d) ID-ul utilizatorului, care a solicitat informaţia.

Secţiunea 11
Asigurarea protecţiei contra programelor dăunătoare (viruşilor). Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

73. Protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal este asigurată prin existenţa programelor licențiate antivirus.
74. Se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

Secţiunea 12
Gestionarea incidentelor de securitate

75. Personalul/angajații [se indică localitatea] care asigură exploatarea sistemelor informaţionale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.
76. Personalul/angajații [se indică localitatea] informează neîntîrziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

77. Prelucrarea incidentelor include: depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.
78. Pînă la data de 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova despre incidentele de securitate constatate.
79. În cazul producerii incidentelor de securitate în cadrul [se indică localitatea], persoana responsabilă din cadrul [se indică localitatea] va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova.
80. În cadrul controalelor efectuate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar şi va fi asigurat accesul la informaţiile necesare relevante obiectului controlului.

Secţiunea 13
Marcarea documentelor.
Responsabilitatea pentru asigurarea securităţii datelor cu caracter personal precum şi a informaţiilor cu accesibilitate limitată

81. Toată informaţia care se intenţionează a fi dezvăluită, şi care conţine date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidenţă al operatorilor de date cu caracter personal.
Model: „Atenţie! Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr. 0000537-00X, înregistrat în Registrul de evidenţă al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal”.
82. Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terţe după caz, pentru nerespectarea dispoziţiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravenţională (art. 741 Cod contravenţional) şi penală (art. 177, art. 178, art. 180 Cod penal).

Anexa nr.4
la Hotărîrea Guvernului
nr.___ din _____

Modelul
Regulamentului de utilizare a datelor cu caracter personal

CONSILIUL
[se indică denumirea completă a consiliului]
D E C I Z I E
Nr. [numărul deciziei] din [data deciziei]

În scopul executării prevederilor Legii nr. 133 din 18.07.2011 privind protecţia datelor cu caracter personal şi a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14.12.2010,

DECIDE:

1. Se aprobă Regulamentul privind asigurarea securităţii datelor cu caracter personal (se anexează);
2. Controlul executării prezentului ordin se pune în sarcina [se indică persoana responsabilă]

Președinte [se indică numele președintelui Consiliului sau ședinței]
Contrasemnează: [se indică numele secretarului]

Anexă unică
la Decizia Consiliului *[se indică denumirea completă a consiliului]*
nr.*[numărul deciziei]* din *[data deciziei]*

Regulament
privind asigurarea securităţii datelor cu caracter personal

I. Dispoziţii generale

1. Regulamentul privind asigurarea securităţii datelor cu caracter personal din cadrul Sistemului informațional automatizat pentru gestionarea și eliberarea actelor permisive (în continuare - Regulament) este elaborat în vederea executării Legii nr. 133 din 18.07.2011 privind protecţia datelor cu caracter personal, Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14.12.2010, Ordinului I.P. ”Agenția Servicii Publice” nr.101 din 09.10.2017 ”Cu privire la aprobarea Politicii în domeniul securității datelor cu caracter personal a Instituției publice ”Agenția Servicii Publice”.

2. Sistemul informațional automatizat pentru gestionarea și eliberarea actelor permisive (în continuare – SIA GEAP) a fost creat în vederea executării prevederilor Hotărârii Guvernului nr.550 din 13.06.2018 „Cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat de gestionare și eliberare a actelor permisive” și Hotărârii Guvernului nr.551 din 13.06.2018 „Pentru aprobarea Regulamentului cu privire la modul de ținere a Registrului actelor permisive” [*se va include prezenta hotărîre de Guvern după publicare*].

3. Prezentul Regulament defineşte următoarele noţiuni:
date cu caracter personal – orice informaţie referitoare la o persoană fizică, care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;
autentificare – verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;
identificare – atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;
integritate – certitudinea, necontradictorialitatea şi actualitatea informaţiei, care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;
mijloace de protecţie criptografică a informaţiei, care conţine date cu caracter personal – mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează

algoritmi de conversie criptografică a informaţiei, care conţine date cu caracter personal, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;
sesiune de lucru – perioada, care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale şi până la momentul opririi acestora;
utilizator – persoana, care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;
sistem informaţional de date cu caracter personal – totalitatea resurselor şi tehnologiilor informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie, care conţine date cu caracter personal;
NIAC - acțiune a deponentului notificării privind inițierea activității de comerț (NIAC) prin SIA GEAP sau pe suport de hârtie conform Legii nr. 231 din 23.09.2010 cu privire la comerțul interior. Operarea cu NIAC este egalată cu operarea actului permisiv, în partea în care nu contravine legii prenotate și altor acte normative în vigoare.

4. Prezentul Regulament stabileşte cerinţele minime necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în procesul ţinerii Registrului actelor permisive, care este format de către SIA GEAP, în conformitate cu prevederile Hotărârii Guvernului nr.550 din 13.06.2018 „Cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat de gestionare și eliberare a actelor permisive”.

5. În SIA GEAP datele cu caracter personal se prelucrează în scopul:
1) evidenţei centralizate automatizate unice a actelor permisive eliberate de către autorităţile emitente indicate în Nomenclatorul actelor permisive eliberate de către autorităţile emitente persoanelor fizice şi persoanelor juridice pentru practicarea activităţii de întreprinzător, aprobat prin anexa nr.1 la Legea nr. 160 din 22 iulie 2011 privind reglementarea prin autorizare a activităţii de întreprinzător și Legii nr. 231 din 23.09.2010 cu privire la comerțul interior;
2) înregistrării actelor permisive și asigurării consultării şi obținerii extraselor din Registrul actelor permisive de către autoritățile publice, persoanele fizice și agenții economici din Republica Moldova;
3) asigurării formării resursei informaţionale de stat privind actele permisive;
4) asigurării sistemelor informaţionale departamentale cu date complete şi veridice referitoare la actele permisive eliberate de autoritățile competente.

II. Categoria datelor cu caracter personal şi a sistemului de prelucrare a acestora

6. În conformitate cu prevederile punctelor 10 și 11 din Regulamentul cu privire la modul de ținere a Registrului actelor permisive aprobat prin Hotărârea Guvernului nr.551 din 13.06.2018, înregistrarea de stat a actelor permisive intră în atribuția autorităților emitente de acte permisive, iar ținerea Registrului de stat al actelor permisive intră în atribuțiile I.P. „Agenția Servicii Publice”, care prelucrează datele cu caracter personal prin mijloace automatizate.

7. În cadrul I.P. „Agenția Servicii Publice” și autorităților emitente se prelucrează date cu caracter personal ale solicitanților de acte permisive, care se înscriu în Registrul actelor permisive, în conformitate cu prevederile Regulamentului cu privire la modul de ținere a Registrului actelor permisive aprobat prin Hotărârea Guvernului nr.551 din 13.06.2018.

8. În SIA GEAP se prelucrează datele cu caracter personal ale cetăţenilor RM şi cetăţenilor străini solicitanți de acte permisive.

9. În SIA GEAP se prelucrează următoarele date cu caracter personal:
a) IDNP;
b) datele personale de identificare a persoanei: numele, prenumele;
c) date privind domiciliul şi/sau reşedinţa;
d) datele de contact (număr telefon, e-mail).

III. Sursa și modul de obținere a datelor cu caracter personal în SIA GEAP

10. Surse de colectare a datelor cu caracter personal în SIA GEAP sunt:
1) subiectul de date cu caracter personal nemijlocit, prin depunerea cererii de eliberare a actului permisiv;
2) documentele prezentate de către persoană, subiectul de date cu caracter personal, prevăzute de cadrul normativ;
3) sistemele informaționale de date prin intermediul cărora are loc acumularea și actualizarea informației în SIA GEAP:
a) SIA ”Registrul de stat al populației”;
b) SIA „Registrul de stat al unităților de drept”
c) sursele informaționale automatizate ale ASP, care conțin date despre bunurile imobile;
d) Sistemul informațional automatizat „Registrul de stat al unităților administrativ-teritoriale şi al adreselor”;
e) Sistemul informațional automatizat „Contul curent al contribuabilului”;
f) Registrul de stat al transporturilor;
g) Registrul de stat al conducătorilor de vehicule;
h) sursele informaționale automatizate ale Casei Naționale de Asigurări Sociale;
i) sursele informaționale automatizate ale Companiei Naționale de Asigurări în Medicină;
j) sursele informaționale automatizate ale Agenției Naționale pentru Siguranța Alimentelor.

4) Resurse informaționale neautomatizate de date cu caracter personal cum sunt dosarele de autorizare pentru fiecare persoană care a depus cererea pentru eliberarea actului permisiv.

11. Prelucrarea datelor cu caracter personal se efectuează în temeiul consimțământului exprimat de solicitant la depunerea cererii și documentelor necesare pentru eliberarea actului permisiv.

IV. Utilizatorii SIA GEAP

12. Utilizarea SIA GEAP se efectuează în conformitate cu Regulamentul cu privire la modul de ținere a Registrului actelor permisive aprobat prin Hotărârea Guvernului nr.551 din 13.06.2018.

13. Utilizatorii în SIA GEAP sînt:
1) autoritatea emitentă de acte permisive – autoritatea publică centrală/locală care este implicată în eliberarea actelor permisive. Aceasta va procesa cererile și va înregistra în cadrul SIA GEAP datele privind actele permisive eliberate sau refuzate în conformitate cu prevederile Conceptului tehnic al Sistemului informațional automatizat pentru gestionarea și eliberarea actelor permisive și ale prezentului Regulament;
2) solicitantul (persoana fizică/unitatea de drept) al actului permisiv, care completează cererile și anexează documentele scanate;
3) laboratorul, care prezintă rezultatele încercărilor de laborator;

4) Agenția Servicii Publice (centre multifuncționale) – instituție publică care va înregistra toate tipurile de acte permisive și care va completa formularele de cerere cu anexarea documentelor privind solicitarea actului permisiv, inclusiv cu eliberarea actului permisiv.

V. Identificarea, autentificarea şi administrarea accesului utilizatorului în SIA GEAP

14. Managementul utilizatorilor în cadrul Registrului actelor permisive și procesele de administrare sunt stabilite în Capitolul V din Regulamentul cu privire la modul de ținere a Registrului actelor permisive aprobat prin Hotărârea Guvernului nr.551 din 13.06.2018.

VI. Restricţii la utilizarea datelor cu caracter personal în cadrul SIA GEAP

15. Destinatarii datelor Registrului actelor permisive vor avea acces la informația privind actele permisive cu respectarea legislației în domeniul protecției datelor cu caracter personal.

16. Agenția Servicii Publice este obligată să monitorizeze utilizarea datelor din Registrul actelor permisive în modul stabilit de legislația în vigoare. Utilizarea, difuzarea sau modificarea ilegală a datelor ori nimicirea lor se sancționează în conformitate cu legislația în vigoare.

17. Asigurarea securităţii, confidenţialităţii şi integrităţii datelor prelucrate în cadrul Registrului actelor permisive se efectuează cu respectarea strictă a cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale, aprobate prin hotărîre de Guvern.

18. Regimul juridic de utilizare a datelor din Registrul actelor permisive este stabilit în Capitolul IV din Regulamentul cu privire la modul de ținere a Registrului actelor permisive aprobat prin Hotărârea Guvernului nr.551 din 13.06.2018.

VII. Înștiințarea și informarea subiectului privind prelucrarea datelor cu caracter personal din SIA GEAP

19. Subiectul datelor cu caracter personal se informează despre accesarea datelor cu caracter personal în SIA GEAP prin intermediul unui răspuns, în formă scrisă, în cazul unei adresări scrise a subiectului în adresa I.P. „Agenția Servicii Publice”, în conformitate cu art. 13 al Legii nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal şi legislaţia în vigoare.

20. Informarea subiectului se efectuează în conformitate cu Regulamentul cu privire la modul de examinare a adresărilor scrise ale cetăţenilor şi organizaţiilor/instituţiilor în cadrul I.P. „Agenţia Servicii Publice”.

VIII. Acordarea informației persoanelor terțe din SIA GEAP

21. În conformitate cu punctul 42 din Regulamentul cu privire la modul de ținere a Registrului actelor permisive aprobat prin Hotărârea Guvernului nr.551 din 13.06.2018, datele recepţionate din Registrul actelor permisive nu pot fi transmise persoanelor terţe, dacă legislaţia în vigoare sau tratatele internaţionale la care Republica Moldova este parte nu prevăd altfel.

IX. Termenul prelucrării (păstrării) datelor cu caracter personal din SIA GEAP

22. În vederea executării Ordinului I.P. „Agenţia Servicii Publice” nr. 182 din 16.11.2017 ”Cu privire la stabilirea termenelor de stocare a datelor în resursele informaționale din cadrul I.P. „Agenţia Servicii Publice”, termenul prelucrării (păstrării) datelor cu caracter personal din SIA GEAP este nelimitat.
23. Datele de audit privind accesarea informaţiei sunt stocate pe un termen de 2 ani.
24. Datele tehnologice de completare și actualizare a Registrului se stochează pe un termen de 7 ani.
25. Datele de audit privind funcţionarea echipamentului tehnico-aplicativ şi sistemelor informaţionale sunt stocate pe un termen de 1 an.

X. Persoana responsabilă de prelucrarea datelor cu caracter personal din SIA GEAP

26. Administratorii de conținut din cadrul autorităților emitente de acte permisive sunt persoane cu funcţie de răspundere, responsabile pentru colectarea, înregistrarea, organizarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea datelor cu caracter personal în Registrul actelor permisive, în limita competenței autorității emitente.

27. Administratorii de utilizatori din cadrul I.P. „Agenția Servicii Publice” și autorităților emitente de acte permisive sunt persoane cu funcție de răspundere (potrivit competenței), responsabile pentru întocmirea cererilor în vederea acordării accesului la datele cu caracter personal din Registrul actelor permisive şi pentru instruirea acestora în domeniul protecţiei datelor cu caracter personal.

28. Administratorii pentru domeniile de competență din cadrul I.P. „Agenția Servicii Publice” și autorităților emitente de acte permisive de securitate sunt persoane cu funcție de răspundere, responsabile de securitatea şi asigurarea auditului proceselor de prelucrare a datelor cu caracter personal în SIA GEAP, de asigurarea funcționării mijloacelor tehnice și de program (sisteme software și hardware, tehnico-aplicativ, de mentenanță a SIA).

XI. Măsuri pentru asigurarea protecției și securității datelor cu caracter personal din SIA GEAP

29. Măsurile pentru asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în SIA GEAP, se efectuează în conformitate cu Hotărârea Guvernului nr. 1123 din 14.12.2010 privind aprobarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, Conceptul tehnic al SIA GEAP aprobat prin Hotărîrea Guvernului nr.550 din 13.06.2018, Regulamentul cu privire la modul de ținere a Registrului actelor permisive aprobat prin Hotărârea Guvernului nr.551 din 13.06.2018 și Politica de securitate a datelor cu caracter personal a I.P. „Agenţia Servicii Publice”.

30. Modul de realizare a elementelor ciclului de viaţă a sistemelor software, precum şi asigurarea funcţionării mijloacelor tehnice şi de program se efectuează în conformitate cu Regulamentul privind atribuţiile subdiviziunilor participante la administrarea resurselor informaţionale ale I.P. „Agenţia Servicii Publice”.

31. Gestionarea şi configurarea funcţiilor de securitate a SIA GEAP se efectuează de către administratorul de sistem în conformitate cu Regulamentul privind atribuţiile subdiviziunilor participante la administrarea resurselor informaţionale ale I.P. „Agenţia Servicii Publice”.

32. Acordarea accesului utilizatorilor externi la SIA GEAP se efectuează în conformitate cu Regulamentul privind acordarea accesului la resursele informaţionale deţinute de I.P. „Agenţia Servicii Publice” utilizatorilor interni şi externi.

33. Informaţia recepţionată din SIA GEAP se marchează în conformitate cu Cerinţele de marcare a informaţiei de ieşire ce conţine date cu caracter personal în cadrul I.P. „Agenţia Servicii Publice”.

34. Datele cu caracter personal din SIA GEAP sunt confidenţiale. Acordarea informaţiei din SIA GEAP se efectuează în conformitate cu Regulamentul privind acordarea accesului la resursele informaţionale deţinute de I.P. „Agenţia Servicii Publice” utilizatorilor interni şi externi.

35. Acordarea informaţiilor referitoare la prelucrarea datelor cu caracter personal în SIA GEAP se efectuează în conformitate cu Regulamentul „Cu privire la modul de examinare a adresărilor scrise ale cetăţenilor şi organizaţiilor/instituţiilor în cadrul I.P. „Agenţia Servicii Publice” privind auditul operaţiunilor de prelucrare a datelor cu caracter personal”.

36. Copierea de rezervă se efectuează în conformitate cu Regulamentul de funcţionare a platformei tehnologice guvernamentale comune M-cloud.

37. Sunt supuse protecţiei toate resursele informaţionale, care conţin date cu caracter personal, inclusiv:
a) suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;
b) sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi multiplicare a documentelor, alte mijloace tehnice de prelucrare a informaţiei.

38. Protecţia datelor cu caracter personal prelucrate în sistemul informaţional se efectuează prin următoarele metode:
a) preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
b) excluderea accesului neautorizat la datele cu caracter personal prelucrate.

39. Preîntâmpinarea scurgerii de informaţii, care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, inclusiv cu utilizarea măsurilor organizaţionale, tehnice şi de regim.

40. Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea software-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii software-ului şi efectuarea periodică a copiilor de siguranţă.

XII. Securitatea mediului de funcţionare

41. Securitatea mediului de funcţionare reprezintă protecţia fizică a resurselor informaţionale de accesul nesancţionat, deteriorări şi perturbaţii, adică amplasarea lor în încăperi securizate, delimitate de un anumit perimetru al securităţii.

42. Accesul în spaţiile securizate, unde sunt amplasate serverele este restricţionat, fiind permis doar persoanelor, care au autorizaţia necesară, în timpul orelor de program, doar în caz de necesitate şi se interzice aflarea persoanelor terţe.

43. În scopul asigurării securităţii utilajului, acesta este amplasat într-o încăpere aparte la loc vizibil, amenajată cu climatizator puternic, în cutii de metal, minimalizând acţiunile pericolelor obişnuite, artificiale, tehnogene şi naturale.

XIII. Gestionarea incidentelor de securitate din cadrul SIA GEAP

44. Utilizatorii datelor Registrului actelor permisive, în procesul conectării la sistem, în mod obligatoriu, vor trece instruirea de reacţionare la incidentele de securitate informaţională contra semnătură.

45. Utilizatorii şi administratorii utilizatorilor datelor Registrului actelor permisive, în cazul apariţiei incidentelor legate de încălcarea securităţii, sunt obligaţi să informeze neîntârziat subdiviziunea responsabilă din cadrul I.P. „Agenţia Servicii Publice”.

46. Incidentele de securitate în cadrul SIA GEAP vor fi urmărite şi documentate în regim permanent de către subdiviziunea responsabilă, cu utilizarea mijloacelor automatizate de urmărire a incidentelor.

47. Subdiviziunea responsabilă din cadrul I.P. „Agenţia Servicii Publice”, anual, pînă la data de 31 ianuarie, va întocmi raportul despre incidentele de securitate la prelucrarea datelor cu caracter personal, care, după aprobarea de către conducerea Agenţiei, va fi expediat în adresa Centrului Naţional pentru Protecţia Datelor cu Caracter Personal.

XIV. Dispoziţii finale

48. Controlul și responsabilitatea privind modul de ținere a Registrului actelor permisive se stabilește în conformitate cu normele stipulate în Capitolul VII al Regulamentului cu privire la modul de ținere a Registrului actelor permisive aprobat prin Hotărârea Guvernului nr.551 din 13.06.2018.

Nota informativă la proiectul hotărîrii Guvernului
pentru aprobarea soluției de ”ghișeu unic”
pentru implementarea resursei informaționale în domeniul comerțului

1. Denumirea autorului şi, după caz, a participanţilor la elaborarea proiectului

Prezentul proiect de hotărîre este elaborat de către Ministerul Economiei și Infrastructurii.

2. Condiţiile ce au impus elaborarea proiectului de act normativ şi finalităţile urmărite

Temei pentru elaborarea și promovarea proiectului servesc prevederile Legii nr.231/2010 cu privire la comerțul interior. Astfel, art. 3 și art. 15 aliniatul (3), din legea prenotată stipulează că **Guvernul creează și administrează** resursă informaţională de stat în domeniul comerțului, ceea ce presupune asigurarea printre altele și posibilitatea depunerii notificării privind inițierea activității de comerț on-line prin intermediul unui ghișeu unic. Lipsa resursei informaționale și a ghișeului unic în domeniul comerțului împiedică aplicarea completă a prevederilor de procedură privind depunerea notificării stabilite în Legea nr.231/2010 cu privire la comerțul interior.

Scopul proiectului constă în:

1. Realizarea obligației legale a Guvernului de instituire a resursei informaționale în domeniul comerțului și asigurarea depunerii notificării privind inițierea activității de comerț on-line prin intermediul unui ghișeu unic.
2. Prin realizarea scopului primar se asigură implementarea prevederilor legale și soluționarea situației actuale potrivit căruia prevederile Legii nr.231/2010 cu privire la comerțul interior nu sunt aplicate complet, existînd o procedură alternativă vis-a-vis de depunerea notificării privind inițierea activității de comerț prevăzută de art. X alin. (3) din Legea nr. 153/2016 pentru modificarea şi completarea unor acte legislative.

Modalitatea legală prin care Guvernul poate asigura conformarea cadrului legal este adoptarea unei hotărâri de Guvern în acest sens.

Proiectul propus se încadrează în programul guvernării de realizare a reformei cadrului de reglementare a mediului de afaceri: Strategia naţionale de dezvoltare „Moldova 2020”, aprobată prin Legea nr.166 din 11 iulie 2012, cu modificările şi completările ulterioare; Strategia reformei cadrului de reglementare a activităţii de întreprinzător pentru anii 2013-2020, aprobată prin Hotărîrea Guvernului nr.1021 din 16 decembrie 2013; prevederile Legii nr. 231 din 23.09.2010 cu privire la comerţul interior, Legii nr. 160 din 22.07.2011 privind reglementarea prin autorizare a activităţii de întreprinzător, Legii nr. 161 din 22.07.2011 privind implementarea ghişeului unic în desfăşurarea activităţii de întreprinzător, Hotărârii Guvernului nr. 753 din 14.06.2016 pentru aprobarea Conceptului mecanismului de gestionare şi eliberare a actelor permisive şi a Planului de acţiuni privind implementarea soluţiilor de ghişeu unic, Hotărârii Guvernului nr. 550 din 13.06.2018 cu privire la aprobarea Conceptului tehnic al Sistemului informaţional automatizat de gestionare şi eliberare a actelor permisive și Hotărârii Guvernului nr. 551 din 13.06.2018 pentru aprobarea Regulamentului cu privire la modul de ţinere a Registrului actelor permisive.

Resursa informațională și ghișeul unic în domeniul comerțului se vor baza pe platforma SIA GEAP pe baza Hotărârilor de guvern menționate supra, fapt care presupune o resursă deja dezvoltată și operațională, **fără necesitatea elaborării unui soft nou**, a identificării unui dezvoltator, precum și alocării de mijloace financiare suplimentare.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop

armonizarea legislaţiei naţionale cu legislaţia Uniunii Europene

Proiectul hotărîrii de Guvern nu conține norme privind armonizarea legislației naționale cu legislaţia Uniunii Europene.

4. Principalele prevederi ale proiectului şi evidenţierea elementelor noi

Art.3 din Legea nr.231/2010 cu privire la comerțul interior stipulează că Guvernul creează şi administrează resursă informaţională de stat în domeniul comerțului. Scopul urmărit este de a pune în aplicare prevederile Legii nr.231/2010 cu privire la comerțul interior în coraport cu prevederile art. X alin. (3) din Legea nr. 153/2016 pentru modificarea şi completarea unor acte legislative, care statuează că: *(3) Pînă la punerea în funcţiune a resursei informaţionale în domeniul comerţului, comercianţii sînt obligaţi să anexeze la notificarea privind iniţierea activităţii de comerţ:*

a) extrasul din Registrul de stat al persoanelor juridice sau din Registrul de stat al întreprinzătorilor individuali ori, după caz, copia de pe patenta de întreprinzător – în toate cazurile;

b) autorizaţia sanitar-veterinară de funcţionare – în cazul în care desfăşoară activităţile stabilite în anexa nr.3 la Legea nr.231 din 23 septembrie 2010 cu privire la comerţul interior;

c) autorizaţia sanitară de funcţionare – în cazul în care desfăşoară activităţile stabilite în anexa nr.4 la Legea nr.231 din 23 septembrie 2010 cu privire la comerţul interior.

De menționat că, procedură dată este diferită de cea stipulată în art. 14 aliniatele (4) și (5) din Legea nr.231/2010 cu privire la comerțul interior care prevăd anexarea altor acte:

4) La notificarea privind iniţierea activităţii de comerţ se anexează, în anumite cazuri, următoarele acte:

a) actul care confirmă împuternicirile reprezentantului – în cazul în care notificarea este depusă prin intermediul unui reprezentant;

b) copia de pe regulamentul pieţei, adoptat de comerciant, şi copia de pe decizia consiliului local de creare a pieţei – în cazul pieţelor.

(5) În cazul unităţilor de comerţ amplasate nemijlocit pe terenuri proprietate publică, suplimentar actelor stabilite la alin.(4), la notificare se anexează copia de pe actul care confirmă dreptul de proprietate sau folosinţă a terenului pe care este amplasată unitatea comercială (decizia privind atribuirea terenului pentru construcţia şi amenajarea pieţei, titlul de autentificare a dreptului deţinătorului de teren, contractul de arendă/comodat sau, după caz, un alt act).

Cerințele din art. 14 al Legii nr.231/2010 cu privire la comerțul interior fiind exhaustive și mult mai permisive, se axează pe prezumția facilităților oferite de resursa informațională din domeniul comerțului, care presupune că celelalte informații precum datele de identificare al deponentului notificării privind inițierea activității de comerț (în continuare - NIAC), sau orice alte date disponibile pe platforma SIA GEAP, vor fi disponibile prin intermediul resursei informaționale în mod automatizat, din registrele guvernamentale.

Suplimentar, actualmente autoritățile administrației publice locale (în continuare - APL) asigură evidența comercianților care au depus notificarea privind inițierea activității de comerț prin evidențe proprii ceea ce contravine noțiunii de ”*resursă informaţională în domeniul comerţului*” din Legea nr.231/2010 cu privire la comerțul interior, care presupune că resursa va *conține date privind unitățile comerciale și locurile de vînzare* la nivel guvernamental și prevederilor art. 17^9 din legea prenotată care statuează în clar “*Evidenţa şi monitorizarea unităţilor comerciale şi a locurilor de vînzare, precum şi a datelor aferente acestora, se efectuează* ***prin intermediul resursei informaţionale*** *în domeniul comerţului, instituită şi*

administrată de Guvern”.

Noutatea adusă de proiectul hotărârii de Guvern constă în schimbarea situației actuale prin aducerea ei în albia prevederilor legale și racordarea la tendințele actuale de digitizare a proceselor din administrarea afacerilor de comerț din perspectiva “autorizării”, a monitorizării și evidenței acestei activități.

Astfel, comercianții vor avea posibilitatea să aplice cîteva scenarii de depunere a NIAC prin intermediu ghișeului unic:

1) On-line;
2) Prin intermediul APL (off-line).

Ambele scenarii oferă posibilitatea utilizării ghișeului unic în calitate de punct unic de acces pentru solicitarea de acte permisive aferente unor activități de comerț de la autoritățile emitente precum ar fi Agenția Națională pentru Siguranța Alimentelor (ANSA) sau Agenția Națională pentru Sănătate Publică (ANSP) conform Anexelor nr 3 și 4 la Legea nr.231/2010 cu privire la comerțul interior.

Prin oferirea de alternative (on-line și off-line) Guvernul asigură transpunerea în practică a obiectivelor de reducere a contactelor fizice dintre comerciant și funcționar și a costurilor de practicare a afacerii. Efectuarea unei singure vizite în locul a 4 este o economie evidentă pentru business. Drept argumentare poate servi un exemplu simplu – depunerea notificării pentru desfășurarea activității cu codul CAEM 46.32 în care s-ar presupune 2 vizite la ANSA pentru obținerea autorizației de funcționare, o vizită la APL pentru depunerea NIAC și una la Agenția pentru supraveghere Tehnică (AST) pentru informare. În varianta în care s-ar presupune că comerciantul s-ar adresa inițial la APL pentru obținerea de informații relevante – poate fi adăugată o viziă. Astfel, urmare a adoptării prezentului proiect numărul vizitelor se va reduce de la 5 la 1.

Pentru asigurarea dreptului APL de a institui cerințe speciale și interdicții de practicare a comerțului pe teritoriul localității respective și asigurării funcționalități legale a sistemului TI pe baza de SIA GEAP prin asigurarea respectării cadrului legal de operare cu date de caracter personal, proiectul instituie:

a) Modelul Regulamentului de desfăşurare a activităţilor de comerţ în localitate, conform anexei nr. 2.

b) Modelul Politicii în domeniul utilizării datelor cu caracter personal, conform anexei nr. 3;

c) Modelul Regulamentului de utilizare a datelor cu caracter personal, conform anexei nr. 4.

Modificarea Conceptului tehnic al Sistemului informaţional automatizat de gestionare şi eliberare a actelor permisive aprobat prin Hotărârea Guvernului nr. 550 din 13.06.2018 se impune din următoarele motive:

- NIAC nu este un act permisiv, ceea ce comportă specific legat de procedura stabilită de Legea nr.231/2010 cu privire la comerțul interior pentru NIAC vis-a-vis de Legea nr. 160 din 22.07.2011 privind reglementarea prin autorizare a activităţii de întreprinzător pentru actele permisive, precum ar fi spre exemplu lipsa cererii de eliberare, lipsa principiului aprobării tacite, diferența dintre blanchetele utilizate și circuitul mesajelor operate în SIA GEAP, etc;
- Lipsa reflectării în Conceptul tehnic al Sistemului informaţional automatizat de gestionare şi eliberare a actelor permisive aprobat prin Hotărârea Guvernului nr. 550 din 13.06.2018 a noțiunilor de bază din Legea nr.231/2010 cu privire la comerțul interior privind gestionarea NIAC;
- Lipsa fundamentării în cadrul normativ a instituirii și specificului resursei

informaționale în domeniul comerțului, distorsionează aplicarea funcționalității aferentă NIAC din cadrul SIAGEAP, deja elaborată și testată.

5. Fundamentarea economico-financiară

Conform celor descrise de mai sus, adoptarea prezentului proiect nu comportă cheltuieli pentru business, oferind doar beneficii. Din perspectiva bugetului de stat, cheltuielile se înglobează în cadrul celor suportate la realizarea ghișeului unic SIA GEAP pentru implementarea reformei regulatorii.

Dezvoltarea unui nou sistem ar genera cheltuieli enorme pentru bugetul de stat.

Din partea autorităților publice centrale și locale se vor cere îndeplinirea următoarelor acţiuni:

a) să asigure acces la Internet;

b) să asigure completarea fișei postului a persoanei/persoanelor responsabile, cu sarcini de operare în SIA GEAP;

b) să dețină dispozitive tehnice (computer și scanner);

c) să dețină chei electronice compatibile cu serviciul guvernamental de acces M-Pass, pentru angajații care nu sunt funcționari publici, în cazul în care li se va oferi drept de a opera în SIAGEAP;

d) să asigure formalizarea contractelor cu Agenția de Guvernare Electronică pentru funcționalitatea serviciului de plăți electronice M-Pay.

Reliefăm că, cele menționate în mare parte (în special cele de la literele a)-c)) deja sunt funcționale și incluse în bugetele autorităților, prin urmare nu vor genera cheltuieli neprevăzute semnificative.

În cadrul unei discuții prealabile cu APL-urile s-a constatat că APL-urile sunt dotate în mare parte cu tehnica necesară pentru SIA GEAP cu excepția scanerelor. Menționăm că pentru funcționalitatea SIA GEAP este suficientă deținerea unui scanner cu parametri minimi.(rezoluția optică (dpi) -2400x4800, Depf colors (bit) min. 36, Grading graiy scale min 256, interface USB – 2.0/3.0, format file PDF, JPEC).

Costul estimativ a unui astfel de dispozitiv constituie cca 1000 lei per unitate.

Referitor la asigurarea semnăturii electronice și serviciul M-Pay, menționăm că aceste servicii sunt asigurate gratuit pentru autoritățile publice.

6. Modul de încorporare a actului în cadrul normativ în vigoare

Prezentul proiect de hotărîre nu necesită abrogarea sau elaborarea unor acte normative noi. Modificarea Conceptului tehnic al Sistemului informaţional automatizat de gestionare şi eliberare a actelor permisive aprobat prin Hotărârea Guvernului nr. 550 din 13.06.2018 se impune pentru a introduce în prevederile Conceptului specificul (noțiuni și procedură) de operare cu NIAC conform Legii nr.231/2010 cu privire la comerțul interior vis-a-vis de Legea nr. 160 din 22.07.2011 privind reglementarea prin autorizare a activităţii de întreprinzător, fiind indispensabilă scopului adoptării prezentei hotărâri.

7. Avizarea şi consultarea publică a proiectului

În conformitate cu prevederile Regulamentului Guvernului aprobat prin Hotărîrea Guvernului nr. 610/2018, prezentul proiect se transmite Cancelariei de Stat pentru înregistrare.

Proiectul a fost discutat în ședințe cu reprezentanții Cancelariei de Stat, MEI, reprezentanții APL (mun. Chișinău și CALM) și a experților Băncii Mondiale.

8. Constatările expertizei anticorupţie

Informaţia privind rezultatele expertizei anticorupţie va fi inclusă după recepţionarea raportului de expertiză anticorupţie.

9. Constatările expertizei de compatibilitate
Proiectul hotărîrii de Guvern nu conține norme privind armonizarea legislației naționale cu legislaţia Uniunii Europene.
10. Constatările expertizei juridice
Informaţia referitoare la concluziile expertizei privind compatibilitatea proiectului de hotărîre cu alte acte normative în vigoare, precum şi respectarea normelor de tehnică legislativă va inclusă după recepţionarea expertizei juridice.
11. Constatările altor expertize
Proiectul de hotărîre a Guvernului se încadrează în limita reglementărilor normative și conceptele tehnice existente ce vizează reglementarea activității de întreprinzător, venind cu soluții tehnice de realizare a obligației legale, prin urmare, nu este necesară elaborarea Analizei Impactului de Reglementare (AIR).

Secretar general de stat **Iulia COSTIN**

Ministerul Economiei
și Infrastructurii
al Republicii Moldova

nr. 06/2-10762

24.10.2018

Cancelaria de Stat

Prin prezenta, Ministerul Economiei şi Infrastructurii transmite alăturat cererea pentru înregistrarea proiectului de hotărîre a Guvernului „Pentru aprobarea soluției de ghișeu unic pentru implementarea resursei informaționale în domeniul comerțului".

CERERE

privind înregistrarea de către Cancelaria de Stat a proiectului de hotărîre a Guvernului care urmează a fi anunţat în cadrul şedinţei secretarilor generali de stat

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Tipul şi denumirea proiectului	Proiectul de hotărîre a Guvernului „Pentru aprobarea soluției de ghișeu unic pentru implementarea resursei informaționale în domeniul comerțului".
2.	Autoritatea care a elaborat proiectul	Ministerul Economiei şi Infrastructurii
3.	Justificarea depunerii cererii *(indicaţia corespunzătoare sau remarca precum că proiectul este elaborat din iniţiativa autorului)*	Temei pentru elaborarea proiectului servesc prevederile art. 3 și art. 15 aliniatul (3) din Legea nr.231/2010 cu privire la comerțul interior care stipulează că Guvernul creează și administrează resursă informaţională de stat în domeniul comerțului, ceea ce urmează să asigure printre altele și depunerea notificării privind inițierea activității de comerț on-line prin intermediul unui ghișeu unic. Lipsa resursei informaționale și a ghișeului unic împiedică aplicarea completă a prevederilor de procedură privind depunerea notificării.

Digitally signed by Costin Iulia
Date: 2018.10.25 09:40:07 EEST
Reason: MoldSign Signature
Location: Moldova

Piaţa Marii Adunări Naţionale nr. 1, Chişinău, MD-2012, tel. +373 22 250107, fax +373 22 234064
e-mail: mineconcom@mei.gov.md, Pagina web: www.mei.gov.md

4.	Lista autorităţilor şi instituţiilor a căror avizare este necesară	1. Ministerul Sănătăţii, Muncii şi Protecţiei Sociale; 2. Agenţia Naţională pentru Siguranţa Alimentelor; 3. Primăria municipiului Chişinău; 4. Congresul Autorităților Locale din Moldova; 5. I.P. ”Agenţia Servicii Publice”; 6. I.P. ”Agenţia de Guvernare Electronică”; 7. CNPDCP; 8. Ministerul Justiţiei; 9.Centrul Naţional Anticorupţie
5.	Termenul-limită pentru depunerea avizelor/expertizelor	5 zile lucrătoare
6.	Numele, prenumele, funcţia şi datele de contact ale persoanei responsabile de promovarea proiectului	Iliaş Cezar, consultant principal al Secţiei reglementarea mediului de afaceri şi IMM, Tel.022-250-635, e-mail: cezar.ilias@mei.gov.md
7.	Anexe *(proiectul actului care se solicită a fi înregistrat, nota informativă cu documentele de însoţire)*	1. Proiectul de hotărîre a Guvernului „Pentru aprobarea soluției de ghișeu unic pentru implementarea resursei informaționale în domeniul comerțului”. 2. Nota informativă la proiectul hotărîrii Guvernului „Pentru aprobarea soluției de ghișeu unic pentru implementarea resursei informaționale în domeniul comerțului”.
8.	Data şi ora depunerii cererii	
9.	Semnătura	

Secretar General de Stat **Iulia COSTIN**

Ex. C. Iliaş
tel.022-250-635