

**Nota informativă la proiectul hotărârii Guvernului
cu privire la instituirea resursei informaționale în domeniul comerțului**

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului
Prezentul proiect de hotărâre este elaborat de către Ministerul Economiei și Infrastructurii.
2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile 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 informațională 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 și 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 națională de dezvoltare „Moldova 2020”, aprobată prin Legea nr.166 din 11 iulie 2012, cu modificările și completările ulterioare; Strategia reformei cadrului de reglementare a activității de întreprinzător pentru anii 2013-2020, aprobată prin Hotărârea Guvernului nr.1021 din 16 decembrie 2013; prevederile Legii nr. 231 din 23.09.2010 cu privire la comerțul interior, Legii nr. 160 din 22.07.2011 privind reglementarea prin autorizare a activității de întreprinzător, Legii nr. 161 din 22.07.2011 privind implementarea ghișeului unic în desfășurarea activității de întreprinzător, Hotărârii Guvernului nr. 753 din 14.06.2016 pentru aprobarea Conceptului mecanismului de gestionare și eliberare a actelor permissive și a Planului de acțiuni privind implementarea soluțiilor de ghișeu unic, Hotărârii Guvernului nr. 550 din 13.06.2018 cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat de gestionare și eliberare a actelor permissive și Hotărârii Guvernului nr. 551 din 13.06.2018 pentru aprobarea Regulamentului cu privire la modul de ținere a Registrului actelor permissive. 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. Modificările Hotărârii Guvernului nr. 753 din 14.06.2016 pentru aprobarea Conceptului mecanismului de gestionare și eliberare a actelor permissive și a Planului de acțiuni privind

implementarea soluțiilor de ghișeu unic, sunt dictate de necesitatea lărgirii spectrului de obiecte informaționale pentru care va fi utilizat SIA GEAP. În cazul dat se include notificarea privind inițierea activității de comerț, însă există discuții la nivel de autorități privind includerea și altor funcționalități în platforma SIA GEAP pentru a beneficia de toate funcționalitățile incluse.

Operarea acestor modificări va permite și altor entități să considere SIA GEAP ca o platformă deschisă pentru a fi completată cu alte funcționalități. Este evident că elaborarea conceptuală și modificarea practică a sistemului vor necesita efort de modificare a reglementărilor în vigoare și unul financiar pentru serviciile unui dezvoltator (companie de TI).

În vederea lărgirii înțelesului conceptului adoptat prin Hotărârea Guvernului nr. 753/2016 și a conceptelor și/sau mecanismelor/programelor elaborate în baza/sau pentru acesta, toate funcționalitățile și noțiunile vor fi aplicabile nu doar actelor permissive propriu-zise ci și altor funcționalități privind operarea și asigurarea interoperabilității dintre diverse obiecte informaționale și/sau entități aferente domeniului activității de întreprinzător și domeniilor conexe.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

Proiectul hotărârii de Guvern nu conține norme privind armonizarea legislației naționale cu legislația Uniunii Europene.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

Art.3 din Legea nr.231/2010 cu privire la comerțul interior stipulează că Guvernul creează și administrează resursă informațională 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 și completarea unor acte legislative, care statuează că: (3) *Până la punerea în funcțiune a resursei informaționale în domeniul comerțului, comercianții sînt obligați să anexeze la notificarea privind inițierea activității de comerț:*

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) *autorizația sanitar-veterinară de funcționare – în cazul în care desfășoară activitățile stabilite în anexa nr.3 la Legea nr.231 din 23 septembrie 2010 cu privire la comerțul interior;*

c) *autorizația sanitară de funcționare – în cazul în care desfășoară activitățile stabilite în anexa nr.4 la Legea nr.231 din 23 septembrie 2010 cu privire la comerțul 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 inițierea activității de comerț 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 pieței, adoptat de comerciant, și copia de pe decizia consiliului local de creare a pieței – în cazul piețelor.*

(5) *În cazul unităților de comerț 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 folosință a terenului pe care este amplasată unitatea*

comercială (decizia privind atribuirea terenului pentru construcția și amenajarea pieței, titlul de autentificare a dreptului deținătorului 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 permissive, 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 informațională în domeniul comerțului”* din Legea nr.231/2010 cu privire la comerțul interior, care presupune că resursa va conține date privind unitățile comerciale și locurile de vânzare la nivel guvernamental și prevederilor art. 17⁹ din legea prenotată care statuează în clar *“Evidența și monitorizarea unităților comerciale și a locurilor de vânzare, precum și a datelor aferente acestora, se efectuează prin intermediul resursei informaționale în domeniul comerțului, instituită și 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 câteva 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 permissive 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 funcționalității 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 desfășurare a activităților de comerț 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 informațional automatizat de gestionare și eliberare a actelor permissive 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 activității de întreprinzător pentru actele permissive, 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 informațional automatizat de gestionare și eliberare a actelor permissive 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 SIA GEAP, 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 acțiuni:

- 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 SIA GEAP;
- 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 hotărâre nu necesită abrogarea sau elaborarea unor acte normative noi. Modificarea Conceptului tehnic al Sistemului informațional automatizat de gestionare și eliberare a actelor permissive 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 activității de întreprinzător, fiind indispensabilă scopului adoptării prezentei hotărâri.
7. Avizarea și consultarea publică a proiectului
În conformitate cu prevederile Regulamentului Guvernului aprobat prin Hotărârea Guvernului nr. 610/2018, prezentul proiect a fost transmis Cancelariei de Stat pentru înregistrare, fiind înregistrat cu nr. 92/MEI/2018. Urmare demersului Cancelariei de Stat nr.18-23-8807 din 25.10.2018 acesta a fost plasat pe pagina electronica a MEI https://mei.gov.md/transparența/tarnsparența_decizională/anunțuri privind consultările publice/ . Proiectul a fost discutat în ședințe cu reprezentanții Cancelariei de Stat, MEI, reprezentanții APL (mun. Chișinău și CALM) și cu experții Băncii Mondiale.
8. Constatările expertizei anticorupție
A fost primit avizul preventiv cu unele propuneri și observații care au fost luate în considerare. Informația privind rezultatele expertizei anticorupție va fi inclusă după recepționarea raportului de expertiză anticorupție.
9. Constatările expertizei de compatibilitate
Proiectul hotărîrii de Guvern nu conține norme privind armonizarea legislației naționale cu legislația Uniunii Europene.
10. Constatările expertizei juridice
În cadrul expertizei juridice sub aspectul regulilor de tehnică legislativă au fost înaintate unele propuneri și obiecții, care au fost incluse în Sinteza obiecțiilor și propunerilor (recomandărilor).
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

GUVERNUL REPUBLICII MOLDOVA**HOTĂRÂRE**

nr. _____
din _____ 2018

Cu privire la instituirea resursei informaționale în domeniul comerțului

În vederea realizării Strategiei naționale de dezvoltare „Moldova 2020”, aprobate prin Legea nr.166/2012 (Monitorul Oficial al Republicii Moldova, 2012, nr.245-247, art.791), cu modificările ulterioare și a prevederilor art. 17⁹ al Legii nr. 231/2010 cu privire la comerțul interior (Monitorul Oficial al Republicii Moldova, 2016, nr.265-267, art.571), cu modificările ulterioare, Guvernul,

HOTĂRĂȘTE:**1. Se aprobă:**

a) Modificările și completările la Conceptul Tehnic al Sistemului informațional automatizat de gestionare și eliberare a actelor permissive aprobat prin Hotărârea Guvernului nr. 550/2018 cu privire la aprobarea Conceptului tehnic al Sistemului Informațional automatizat de gestionare și eliberare a actelor permissive (în continuare - SIA GEAP), conform anexei nr.1;

b) Modificările și completările la Conceptul mecanismului de gestionare și eliberare a actelor permissive aprobat prin Hotărârea Guvernului nr. 753/2018 pentru aprobarea Conceptului mecanismului de gestionare și eliberare a actelor permissive și a Planului de acțiuni privind implementarea soluțiilor de ghișeu unic, conform anexei nr.2;

c) Modelul Regulamentului de desfășurare a activităților de comerț în localitate, conform anexei nr. 3;

d) Modelul Politicii de securitate a datelor cu caracter personal, conform anexei nr. 4;

e) Modelul Regulamentului privind prelucrarea datelor cu caracter personal în cadrul resursei informaționale în domeniul comerțului, conform anexei nr. 5.

2. Se instituie și se pune la dispoziția Autorităților administrației publice locale și centrale resursa informațională în domeniul comerțului, pe baza SIA GEAP.

3. Autoritățile publice implicate în implementarea soluțiilor 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 ghișeu unic de tip mixt și resursei informaționale în domeniul comerțului în baza SIA GEAP;

b) desemnează persoanele care vor opera în SIA GEAP la nivel de entitate și asigură investirea acestora cu drepturi de utilizare a serviciului electronic guvernamental de autentificare și control al accesului (MPass);

c) formalizează contractual, în conformitate cu reglementările în vigoare, funcționalitatea serviciului guvernamental de plăți electronice (MPay);

asigură, după caz, realizarea măsurilor ce se impun pentru conectarea sistemelor și registrelor

d) informaționale proprii folosite în procesul operării cu NIAC și/sau emiterii actelor permissive la platforma de interoperabilitate (MConnect);

utilizează SIA GEAP în calitate de ghișeu unic în domeniul comerțului și actelor permissive.

4. Se recomandă Autorităților administrației publice locale adoptarea Regulamentului de desfășurare a activităților de comerț în localitate, conform modelului din anexa nr. 3, până la data intrării în vigoare a prezentei hotărâri.

5. Prezenta Hotărâre intră în vigoare după cum urmează:

a) pentru Agenția Națională pentru Sănătate Publică și Agenția Națională pentru Siguranța Alimentelor, autoritățile administrației publice locale ale municipiilor - la expirarea a 60 de zile de la data publicării;

b) pentru autoritățile administrației publice locale ale orașelor, comunelor și satelor și unitatea teritorială autonomă Găgăuzia - la expirarea a 90 de zile de la data publicării.

PRIM-MINISTRU

Pavel FILIP

Contrasemnează:

Ministrul economiei și infrastructurii

Chiril GABURICI

**Modificările și completările la Conceptului tehnic
al Sistemului informațional automatizat
de gestionare și eliberare a actelor permise aprobat prin Hotărârea Guvernului nr.
550/2018**

1. Se completează cu pct. 6¹ - 6³ cu următorul cuprins:

”6¹ Sistemul informațional automatizat de gestionare și eliberare a actelor permise (SIA GEAP), propus în prezentul Concept va servi și ca platformă pentru a realiza prevederile legale de instituire a unei resurse informaționale în domeniul comerțului și a ghișeului unic pentru depunerea notificării privind inițierea activității de comerț (NIAC), va contribui la facilitarea procesului de depunere a NIAC atât pentru persoane, cât și pentru APL. Se propune ca toate APL să utilizeze un singur sistem informațional pentru gestionarea procesului de recepționare a NIAC și a cererilor de eliberare a actelor permise, comunicare și schimb de informații între autoritățile publice implicate în eliberarea actelor permise, standardizarea unor procese de prelucrare a cererilor și recepționare a NIAC și eliberare a confirmării de recepționare a NIAC. Autoritățile emitente de acte permise/APL care utilizează în procesul de gestionare a actelor permise/NIAC altfel de sisteme informaționale (proprie), în cazul în care vor decide păstrarea acestora, implementează soluții compatibile cu SIA GEAP pentru a permite depunerea NIAC/cererilor în format electronic, operarea cu alte obiecte informaționale și cu stocarea lor în Registrul actelor permise al Republicii Moldova (RAP), în vederea asigurării utilizării SIA GEAP ca platformă unică în acest sens.

6² SIA GEAP va servi drept bază pentru ghișeul unic de gestionare NIAC și va integra cele mai moderne instrumente de tehnologii informaționale pentru ca antreprenorii să economisească timp, bani și eforturi administrative la depunerea NIAC, solicitarea și obținerea actelor permise aferente. SIA GEAP va servi drept punct central pentru interconectarea APL și coordonarea activităților lor, astfel ca instituțiile și entitățile implicate să poată face schimb de informații pentru a minimiza cantitatea de informații livrată de deponenți/solicitanți în vederea obținerii actelor permise.

6³ Utilizarea unui sistem informațional unic pentru depunerea și gestionarea NIAC, în afară de beneficiile și funcționalitățile menționate mai sus, va permite stabilirea unui mecanism pentru monitorizarea performanței autorităților publice locale în procesul de gestionare a NIAC și identificarea soluțiilor de optimizare în vederea îmbunătățirii și facilitării gestionării NIAC.”

2. Pct.9 se completează cu următoarele noțiuni:

”NIAC - document recepționat de SIA GEAP prin care autoritatea recepționară constată unele fapte juridice și notificarea întrunirii condițiilor stabilite de lege de către deponent, atestând asumarea de către acesta a unei serii de drepturi și de obligații privind inițierea, desfășurarea și/sau încetarea activității de comerț;

depunerea NIAC - acțiuni a comerciantului (deponentului) operate prin SIA GEAP, sau pe suport de hârtie privind inițierea activității de comerț în baza Legii nr. 231/2010 cu privire la comerțul interior;

deponent NIAC - persoană fizică sau juridică care depune NIAC;

APL - autoritatea administrației publice locale;

administrator - persoana împuternicită de subiecții raporturilor juridice ai SIA GEAP în vederea mentenanței funcționalităților SIA GEAP.”

3. Pct. 10 - 12 vor avea următorul cuprins:

”10. SIA GEAP înglobează posibilitățile funcționale de gestionare a fluxurilor documentare, schimbul de informații, funcțiile de înștiințare, depozitare a datelor și aplicare online, necesare pentru solicitarea și eliberarea actelor permissive, pentru depunerea și gestionarea NIAC sau oricărui alte documente prevăzute de lege.

11. RAP este un registru public care se ține în scopul înregistrării actelor menționate la pct. 10, precum și pentru a asigura informarea și obținerea extraselor din el de către autoritățile publice, persoanele fizice și agenții economici din Republica Moldova. RAP va fi parte integrantă a resurselor informaționale de stat.

12. SIA GEAP va pune la dispoziția solicitanților următoarele servicii:

În domeniul actelor permissive:

1) obținerea actelor permissive prin intermediul portalului guvernamental unic al serviciilor publice <https://servicii.gov.md>;

2) asigurarea accesului la toate informațiile necesare pentru obținerea actelor permissive;

3) depunerea on-line a cererii pentru obținerea actelor permissive;

4) depunerea on-line a cererii pentru obținerea documentelor necesare pentru actele permissive;

5) achitarea on-line a taxelor pentru obținerea actelor permissive;

6) schimbul electronic de informații legate de actele permissive între autorități și sistemele lor TI;

7) semnarea electronică a documentelor.

În domeniul NIAC:

1) depunerea NIAC on-line prin intermediul portalului guvernamental unic al serviciilor publice <https://servicii.gov.md>;

2) asigurarea accesului la toate informațiile necesare pentru depunerea NIAC;

3) depunerea on-line a cererii pentru obținerea actelor permissive lipsă sau oricărui alte documente prevăzute de lege necesare NIAC;

4) depunerea on-line a documentelor necesare pentru NIAC;

5) achitarea on-line a taxelor pentru depunerea NIAC și obținerea actelor permissive;

6) schimbul electronic de informații legate de actele permissive între autorități și sistemele lor TI;

7) semnarea electronică a documentelor;

8) stocarea informațiilor despre NIAC și acte permissive lipsă .”

4. Pct. 15 se completează cu următoarele subpuncte cu următorul cuprins:

”23) Legea nr. 231/2010 cu privire la comerțul interior;

24) Legea nr. 153/2016 cu privire la modificarea și completarea unor acte legislative.”

5. Pct. 18 se modifică după cum urmează:

a) subpunctul 2) se completează cu o literă nouă cu următorul cuprins:

”d) deponenților NIAC. ”.

b) se completează cu un subpunct nou cu următorul cuprins:

”4) Conturul funcțional „NIAC” include funcții de evidență a:

a) NIAC;

b) actelor permissive lipsă aferente NIAC;

c) deciziilor de refuz de recepționare a NIAC;

d) deciziilor de suspendare a NIAC;

e) notificărilor de încetare a NIAC;

- f) modificarea datelor din NIAC;
- g) refuzul (temeiurile) de acceptare NIAC;
- h) înștiințările de recepționare a NIAC.

6. Punctul 22 va avea următorul cuprins:

”22. Registratorii SIA GEAP sînt autoritățile administrației publice locale, conform Legii nr. 231/2010 cu privire la comerțul interior, autoritățile emitente de acte permissive, indicate în Nomenclatorul actelor permissive eliberate de către autoritățile emitente persoanelor fizice și juridice pentru practicarea activității de întreprinzător (în continuare – *Nomenclator*), aprobat prin anexa nr.1 la Legea nr.160/2011 privind reglementarea prin autorizare a activității de întreprinzător, care introduc datele în legătură cu eliberarea actelor permissive indicate în Nomenclator și operează cu NIAC sau cu alte obiecte informaționale pe platforma SIA GEAP.”

7. Punctele 24 și 25 vor avea următorul cuprins:

”24. Documentele de intrare sînt următoarele:

- 1) cereri;
- 2) rapoarte de încercări de laborator;
- 4) anexe la cereri;
- 5) documente scanate în format PDF, JPG necesare în procesul de solicitare a actului permisiv;
- 6) NIAC;
- 7) alte obiecte informaționale.

25. Documentele de ieșire sunt următoarele:

- 1) NIAC;
- 2) acte permissive;
- 3) decizie de eliberare a actului permisiv;
- 4) decizie de refuz de eliberare a actului permisiv;
- 5) rapoarte ce conțin informații despre actul permisiv/NIAC;
- 6) rapoarte statistice privind NIAC și actele permissive solicitate/emise;
- 7) notificare (de admitere, de refuz);
- 8) înștiințare de recepționare NIAC;
- 9) înștiințare privind refuzul de recepționare NIAC;
- 10) notificarea de încetare NIAC;
- 11) notificarea de modificare a datelor din NIAC.”

8. Pct. 27 subpunctul 3) se completează cu următoarele:

cerere pentru un act permisiv lipsă - document privind solicitarea unui act permisiv care se completează de către solicitant sau APL în format electronic sau pe suport de hârtie conform scenariilor prevăzute în prezentul Concept;

înștiințare de recepționare a NIAC - mesaj electronic emis de către SIA GEAP pe adresa electronică specificată de deponent, pentru confirmarea recepționării NIAC. Înștiințarea de recepționare a NIAC recepționată în regim on-line va fi emisă în termen de cel mult 3 zile lucrătoare, în temeiul aliniatului (3) al art. 16 din Legea nr. 231/2010 cu privire la comerțul interior;

notificare de acceptare - mesaj electronic emis de către SIA GEAP pe adresa electronică specificată de solicitant, ce conține informații referitoare la acceptarea cererii privind solicitarea unui act permisiv lipsă;

înștiințare privind refuzul - mesaj emis de către SIA GEAP ce conține informații referitoare la refuzul de recepționare 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 autorității publice responsabil de prelucrarea datelor privind NIAC sau un act permisiv, ce conține informații privind înregistrarea unei noi cereri;

notificare privind statutul NIAC - mesaj emis de către SIA GEAP adresat deponentului, ce conține informații privind statutul NIAC;

NIAC - document electronic sau imprimat conform unui model prestabilit, recepționat/emis de SIA GEAP căruia i se atribuie un număr unic, care va servi drept identificator a NIAC pe parcursul întregului flux de procesare și stocare;

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. 231/2010 cu privire la comerțul 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. 231/2010 cu privire la comerțul interior sau acțiune a operatorului în baza cererii scrise a deponentului/solicitantului.”

9. Pct. 28 se completează cu un subpunct nou cu nr. 11) cu următorul cuprins:

”11) identificator al obiectului informațional „NIAC” este codul unic de identificare, generat și atribuit de SIA GEAP, care are următoarea structură:

„P00001/2018”, unde:

P - (tip permit);

00001 - număr;

2018 - anul emiterii;”

10. Pct. 29 se completează cu următoarele subpuncte cu următorul cuprins:

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

Prezentul scenariu este utilizat de către deponenți care au acces la Internet și se pot autentifica pe portalului guvernamental unic al serviciilor publice prin intermediul serviciului electronic guvernamental de autentificare și control al accesului utilizând instrumentele disponibile. Deponenții sunt scutiți de vizitarea autorităților publice responsabile de eliberarea actelor permissive și pot să depună NIAC în format electronic cu anexarea documentelor necesare, de asemenea, în format electronic.

Depunerea NIAC implică următorii pași:

a) accesarea portalului guvernamental unic al serviciilor publice <https://servicii.gov.md> sau a ghișeului unic pentru gestionarea acelor permissive (SIA GEAP, <https://actpermisiv.gov.md>) a serviciului *Notificare privind inițierea activității de comerț*;

b) autentificarea în SIA GEAP prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass), folosind unul din instrumentele disponibile;

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

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

e) anexarea documentelor necesare, după caz;

f) în cazul în care deponentul nu dispune de unele acte (acte permissive, alte acte sau documente) necesare pentru anexare la NIAC, acesta va depune cererea pentru obținerea 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 permissive cu ajutorul Serviciului Guvernamental de Plăți Electronice (MPay), prin transfer bancar sau depunere de numerar. După efectuarea plății, SIA GEAP va primi confirmarea de plată prin MPay sau, în caz contrar, specialistul

responsabil din cadrul autorității emitente va verifica faptul efectuării plății prin alte mijloace (cum ar fi verificarea contului bancar sau ordinului de încasare a numerarului);

h) după ce toate documentele necesare vor fi atașate și formularul completat, deponentul va putea salva NIAC cu statut de „proiect” sau o va putea semna electronic și trimite spre examinare autorității publice locale responsabile, fiind informat despre recepționare printr-o înștiințare de recepționare;

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 permissive lipsă responsabilă, va primi înștiințarea cu privire la NIAC nouă intrată în sistem prin SIA GEAP și/sau e-mail, după caz;

k) în cazul solicitării de acte permissive lipsă, 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 SIA GEAP refuzul de recepționare a NIAC în temeiul aliniatului (3) al art. 16 din Legea nr. 231/2010 cu privire la comerțul interior.

15) *depunerea NIAC la sediul autorității publice locale (off-line)*

Prezentul scenariu va fi utilizat atunci când deponenții vor vizita autoritățile publice locale pentru depunerea NIAC și a cererilor de solicitarea a actelor permissive aferente NIAC, după caz. Acest scenariu implică depunerea NIAC în format de hîrtie la ghișeul APL, și procesarea acesteia și a cererilor de solicitare a actelor permissive 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 autorități și pentru asigurarea transparenței întregului proces de solicitare și eliberare a actelor permissive.

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

a) solicitantul vizitează sediul APL;

b) reprezentantul APL oferă asistență deponentului la completarea corectă a NIAC pe suport de hîrtie, sau direct în sistem;

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 din cadrul APL. Actele, sau informațiile (datele) privind actele care pot fi obținute prin intermediul SIA GEAP vor fi solicitate prin intermediul SIA GEAP, utilizatorul din cadrul APL oferind asistența necesară deponentului/solicitantului acționând aici în calitate de ”front-office sau prezentate pe suport de hîrtie dacă au fost obținute anterior;

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

f) reprezentantul APL completează NIAC și cererea de eliberare a actului permisiv lipsă după caz, anexează documentele scanate sau indică datele de identificare a actelor în SIA GEAP și semnează NIAC și/sau cererea de eliberare a actelor permissive 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 și a documentelor scanate sau obținute într-un alt mod corespund documentelor depuse și semnate de deponent/solicitant. Temei pentru depunerea cererilor de către APL către autoritățile emitente de acte permissive lipsă, din numele deponentului/solicitantului va servi acordul în scris al deponentului/solicitantului consfințit prin înscrierea sintagmei ”*acte suplimentare necesare*” în rubrica Anexe din formularul NIAC cu semnarea olografă sub aceasta;

g) în cazul în care deponentul semnează olograf NIAC dar nu anexează actele permise obligatorii desfășurării activității de comerț din NIAC și nu solicită completarea cererii de eliberare a actului permisiv lipsă, reprezentantul autorității publice semnează electronic NIAC iar SIA GEAP va genera înștiințarea de recepționare NIAC cu remiterea NIAC autorităților emitente de acte permise 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 permise, 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 Plăți Electronice (MPay), prin transfer bancar sau în numerar;

k) după efectuarea plății SIA GEAP va primi confirmarea plății care va fi accesibilă pentru specialistul autorității emitente de acte permise 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 sau serviciul nu este achitat, și va fi transmisă mai târziu, caz în care SIA GEAP nu va genera număr de înregistrare;

m) în cazul în care cererea de eliberare a actelor permise 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 și 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 și cererii după caz, va fi folosit de către APL pentru a monitoriza statutul NIAC și 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 obținerea documentelor lipsă la NIAC constă din următoarele etape:*

a) utilizatorul din cadrul APL completează cererea de obținere a actului permisiv lipsă, o imprimă, iar solicitantul semnează cererea olograf pe suport 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 atașa actul electronic (scanat) sau poate să-l solicite prin utilizarea funcționalităților disponibile;

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

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

f) după obținerea documentelor necesare, solicitantul/utilizatorul din cadrul APL accesează cabinetul personal și deschide proiectul respectiv;

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

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

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

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 declanșează de către specialistul responsabil din cadrul autorității recepționare/emitente a actului permisiv*

Prezentul scenariu constă din următoarele etape:

- a) în baza autosesizării sau notificării SIA GEAP, specialistul din cadrul autorității recepționare/emitente decide privind necesitatea de a accesa dosarul NIAC;
 - b) specialistul din cadrul autorității recepționare/emitente a NIAC accesează dosarul NIAC în SIA GEAP și accesează NIAC respectivă;
 - c) statutul actului permisiv se modifică doar după aprobarea conducerii autorității 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” și anexează documentele necesare în baza cărora (data și numărul deciziei/actului) se efectuează *modificarea/suspendarea/încetarea* NIAC.
 - e) SIA GEAP notifică beneficiarul/posesorul NIAC despre schimbarea statutului.
- 19) *scenariul privind aprobarea tacită a actului permisiv în cazul NIAC:*
- a) aprobarea tacită pentru actele permise lipsă solicitate de către deponentul NIAC prin intermediul APL utilizând SIA GEAP survine în baza Legii nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător și a scenariilor de mai sus aplicabile. Certificatul constatator prevăzut de Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător va fi emis pe adresele electronice ale deponentului NIAC (solicitant pentru actele permise lipsă) și APL corespunzător”.

11. Punctul 30 se completează cu subpunctul 11) cu următorul cuprins:

”11) date privind obiectul informațional „NIAC”:

- a) ID - numărul de identificare;
- b) titlu;
- c) data și 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 vânzare (adresa, tipul (Codul CAEM), suprafața comercială (m²);
- n) pentru unitățile de alimentație publică (capacitatea unității comerciale (numărul de locuri/persoane), inclusiv la terasă (numărul de locuri/persoane),
- o) comercializarea producției alcoolice, comercializarea berii, comercializarea produselor din tutun, desfășurarea comerțului ambulant, comercializarea prin intermediul unității 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 (câmp deschis, sau sintagme solicitării de acte permise lipsă);
- s) Declarația de proprie răspundere și asumarea de obligații;”.

Modificările și completările la Conceptul mecanismului de gestionare și eliberare a actelor permissive aprobat prin Hotărârea Guvernului nr. 753/2018 pentru aprobarea Conceptului mecanismului de gestionare și eliberare a actelor permissive și a Planului de acțiuni privind implementarea soluțiilor de ghișeu unic

1. Pct. 1 se completează cu:

”Datorită complexității procesului de reglementare a activității de întreprinzător, necesității asigurării continuității implementării reformei cadrului de reglementare a activității de întreprinzător, pe platforma MGEAP (SIA GEAP) pot fi dezvoltate sau incluse în acesta orice funcționalități necesare. Prin urmare, în sensul prezentului concept și a conceptelor și/sau mecanismelor/programelor elaborate în baza/sau pentru acesta, toate funcționalitățile și noțiunile sunt aplicabile nu doar actelor permissive propriu-zise ci și altor funcționalități privind operarea și asigurarea interoperabilității dintre diverse obiecte informaționale și/sau entități aferente domeniului activității de întreprinzător și domeniilor conexe.”

2. Pct. 13 se completează cu 2 subpuncte cu următorul cuprins:

”11) depunerea cererilor pentru acte permissive la Agenția Servicii Publice;
12) asigurarea de funcționalități privind operarea și asigurarea interoperabilității dintre diverse obiecte informaționale și/sau entități aferente domeniului activității de întreprinzător și domeniilor conexe.”.

3. Pct. 25:

a) după a doua propoziție se adaugă următoarele:
”Utilizatorii vor opera în sistem după scenariile stabilite. Persoana care solicită eliberarea actului permisiv va alege cel mai potrivit scenariu disponibil într-un caz concret la propria discreție. În cazul când scenariul ales nu este funcțional, MGEAP (SIA GEAP) sau operatorul autorității la care s-a adresat solicitantul, îl vor informa despre scenariul aplicabil.”;

b) la subpunctul 3) sintagma:
”Antreprenorul care depune cererea pe suport de hârtie” se suplinește cu sintagma: ”o poate face la autoritatea publică emitentă a acutului permisiv sau la o altă entitate desemnată în acest sens.”.

MODEL

REGULAMENT
de desfășurare a activității de comerț în
[se indică localitatea]

I. DISPOZIȚII GENERALE

1. Regulamentul de desfășurare a activității 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, protecției vieții, sănătății, securității și intereselor economice și sociale ale cetățenilor.

2. Prezentul Regulament stabilește interdicțiile și cerințele de desfășurare a activității de comerț în [se indică localitatea] în conformitate cu prevederile art.6 alin.(1) lit. n) și alin.(5) din Legea nr.231/2010 cu privire la comerțul interior, în următoarele privințe:

1) interdicția de a desfășura activități de comerț sau anumite forme ale activității de comerț, inclusiv comerțul ambulant, în perimetrul anumitor zone sau străzi ori în intervalul anumitor zile sau ore;

2) modul de desfășurare a activităților de comerț în apropierea edificiilor autorităților publice, instituțiilor de învățământ, instituțiilor medicale, lăcașurilor de cult, monumentelor, lucrărilor de artă, edificiilor cu valoare arhitecturală, istorică sau arheologică, zonelor istorice, precum și în locurile (destinațiile) de interes turistic;

3) distribuirea activităților de comerț între zona centrală și zonele periferice ale localității, precum și între zonele aglomerate și cele neaglomerate;

4) raza în care este interzisă comercializarea producției alcoolice în preajma instituțiilor de învățământ, instituțiilor medicale și lăcașurilor de cult;

5) cerințe privind regimul de lucru (orarul de funcționare) al comercianților în perimetrul anumitor zone sau străzi;

6) interdicția de a comercializa anumite produse sau servicii în perimetrul anumitor zone sau străzi;

7) cerințe privind zonele de parcare de care trebuie să dispună comerciantul la desfășurare a anumitor forme de comercializare.

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

II. INTERDICȚIA DE DESFĂȘURARE A ACTIVITĂȚII DE COMERȚ

4. Se interzice desfășurarea activității de comerț 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. INTERDICȚII PRIVIND DESFĂȘURAREA UNOR FORME DE COMERȚ

Secțiunea 1. Comerțul ambulant

5. 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] .

6. 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

7. 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] .

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

IV. DESFĂȘURAREA ACTIVITĂȚII DE COMERȚ ÎN APROPIEREA EDIFICIILOR ȘI ZONELOR STABILITE DE LEGE

Secțiunea 1. Activitatea de comerț în apropierea unor edificii

9. Activitatea de comerț în perimetrul a [se indică perimetrul (distanța în metri de la edificii)] de la edificiile autorităților publice, instituțiilor de învățămînt, instituțiilor medicale, lăcașurilor 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 comerț în anumite zone

10. Activitatea de comerț în zonele istorice și în locurile (destinațiile) de interes turistic, stabilite de Anexa nr.5, 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] .

V. INTERDICȚII PRIVIND COMERCIALIZAREA UNOR PRODUSE SAU PRESTAREA UNOR SERVICII

Secțiunea 1. Comercializarea producției alcoolice

11. Se interzice comercializarea producției alcoolice în raza a [se indică raza stabilită de APL] din preajma instituțiilor de învățămînt, instituțiilor medicale și lăcașurilor de cult, indicate în Anexa nr.4 la prezentul Regulament.

Secțiunea 2. Jocuri de noroc

12. Se permite/interzice amplasarea sălilor de joc și aparatelor de joc, și desfășurarea jocurilor de noroc, în condițiile stabilite de pct. __, doar 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] .

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

14. 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]

15. 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] .

16. 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.

17. 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]

18. 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] .

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

20. 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 COMERCIANȚILOR

21 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] .

22. 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 desfășurare a activității 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 desfășurare a activității 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 desfășurare a activității 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 desfășurare a activității de comerț în [se indică localitatea]

Lista edificiilor autorităților publice, instituțiilor de învățământ, instituțiilor medicale, lăcașurilor de cult, monumentelor, lucrărilor de artă, edificiilor cu valoare arhitecturală, istorică sau arheologică din [se indică localitatea] (MODEL)

Autorități publice	Adresa
Guvernul Republicii Moldova	Piața Marii Adunări Naționale, 1
Ministerul Afacerilor Interne	Bd. Ștefan cel Mare și Sfânt, nr. 75

Anexa nr.5 la Regulamentul de desfășurare a activității de comerț în [se indică localitatea]

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

Anexa nr.6 la Regulamentul de desfășurare a activității 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 desfășurare a activității 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 desfășurare a activității de comerț în [se indică localitatea]

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

Anexa nr.9 la Regulamentul de desfășurare a activității de comerț în [se indică localitatea]

Străzile și zonele în perimetrul cărora desfășurarea activității de comerț este interzisă în intervalul anumitor ore/zilele.

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

MODEL

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 acționează în baza [se indică actul normativ] și 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 protecția datelor cu caracter personal și cu prevederile Hotărîrii Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

3. La prelucrarea datelor cu caracter personal în cadrul entității sunt aplicate principiile prevăzute de actele internaționale: Declarația universală a drepturilor omului, Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Directiva 95/46/CE a Parlamentului European și a Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, și a celor naționale: Constituția Republicii Moldova, Legea nr.133 din 08.07.2011 privind protecția datelor cu caracter personal, Legea nr.982 din 11.05.2000 privind accesul la informație, Hotărîrea Guvernului nr.1123 din 14 decembrie 2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin, Hotărîrea Guvernului nr.296 din 15 mai 2012 privind aprobarea Regulamentului Registrului de evidență al operatorilor de date cu caracter personal, precum și alte acte normative de profil.

II. Noțiuni generale

4. În prezenta Politică de securitate, sînt definite/utilizate următoarele noțiuni:

date cu caracter personal - orice informație 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 identității 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, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancțiunile contravenționale;

operator - persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau

împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;

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

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

control de securitate - acțiuni întreprinse de către [se indică localitatea] în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;

fișiere temporare - ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat până la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;

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

integritate - certitudinea, necontradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;

mijloace de protecție criptografică a informației care conține date cu caracter personal - mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicații;

nivel de protecție - nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor, elaborat și actualizat corespunzător nivelului dezvoltării tehnologice și 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 și trăsăturilor de protecție selectate pentru securitatea datelor, ținându-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile la care sînt expuse acestea;

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

persoana responsabilă de politica de securitate a datelor cu caracter personal - persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;

protecția informației contra acțiunilor neintenționate - ansamblu de măsuri a acțiunilor neintenționate, provocate de erorile utilizatorului, inico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține date cu caracter personal;

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

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

tehnologie informațională - totalitatea metodelor, procedeele și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;

utilizator - persoana care acționează sub autoritatea deținătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal;

sesiune de lucru - perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și până la momentul opririi acestora;

sistem informațional de date cu caracter personal - totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal;

prelucrarea datelor cu caracter personal - orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, 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, ștergerea sau distrugerea;

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

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

consimțământul subiectului datelor cu caracter personal - orice manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor 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 încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane doar în condițiile unei fizice identificate sau identificabile ori să permită atribuirea investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă.

III. Obiectivele Politicii de securitate a datelor cu caracter personal

5. Obiectivele principale ale Politicii sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv a datelor cu caracter personal prelucrate de [se indică localitatea], atât în cadrul prelucrării manuale, cât și în cadrul sistemelor și proceselor de tehnologie informațională.

6. Securitatea reprezintă o componentă esențială a derulării optime a proceselor bazate pe TI în cadrul [se indică localitatea]. Baza unei securități TI adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv a datelor cu caracter personal, a sistemelor și proceselor TI împotriva influențelor naturale, erorilor umane și tehnice, precum și împotriva acțiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației.

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

8. [se indică localitatea] va proteja datele cu caracter personal atât a participanților la proces/vizitatori, cât și a angajaților săi.

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

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

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

1) preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

- 2) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
- 3) neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- 4) eficientizarea resurselor informaționale atât pe suport de hârtie cât și cel în format electronic.

V. Metodele de protecție a datelor cu caracter personal prelucrate în sistemele informaționale

11. Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:

- 1) preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- 2) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- 3) preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- 4) preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor precum și a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- 5) preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea canalelor VPN;
- 6) preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță;
- 7) scurgerii de informații care conțin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent;
- 8) stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atât cât și pentru cei externi.

VI. Resursele informaționale supuse principiilor de protecție a datelor cu caracter personal

12. Protecția 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 și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

13. Sînt supuse protecției prin mijloace/procedee specifice, toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate pe:

- 1) suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
- 2) sistemele informaționale, rețelele, sistemele operaționale, sistemele de date și alte aplicații, sistemele de telecomunicații, inclusiv are și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

VII. Dispoziții privind ierarhia și obligațiile persoanei responsabile de Politica de securitate a datelor cu caracter personal

14. Operatorul de date cu caracter personal reieșind din specificul activității, prin prezenta Politică de securitate, transpune procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență gestionate.

15. Politica de securitate a datelor cu caracter personal se va revizui cel puțin o dată în an ca rezultat al modificărilor sau reevaluării competențelor entității, 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 cunoștință, sub semnătură, tuturor angajaților responsabili de prelucrarea datelor cu caracter personal, înainte acordării accesului la prelucrarea datelor cu caracter personal, inclusiv și la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecție a datelor cu caracter personal.

17. Responsabil de implementarea și monitorizarea respectării prevederilor datelor cu caracter personal, va fi desemnată persoana care conform fișei postului și/sau ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament și buget) și va avea acces liber la informația necesară pentru îndeplinirea funcțiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

18. Persoana responsabilă desemnată, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor Politicii de securitate, se va subordona nemijlocit conducătorului [se indică localitatea] sau persoanei care îndeplinește interimatul funcției.

19. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilități cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare și prelucrare), precum și 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 acțiuni:

- 1) definește clar responsabilitățile și procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională și de funcționare generală;
- 2) asigură măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal;
- 3) elaborează procedurile de clasificare a informației care conține date cu caracter personal, astfel încât să fie posibil de întocmit un nomenclator și toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date;
- 4) instruește persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

VIII Procedurile organizatorice și tehnice la prelucrarea datelor cu caracter personal

Secțiunea 1

Măsurile generale de administrare a securității informaționale

21. Măsurile generale de administrare a securității informaționale sunt următoarele:

- 1) în cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.
- 2) Computerele, terminalele de acces și imprimantele sînt deconectate la terminarea sesiunilor de lucru.
- 3) Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.
- 4) Este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acestora de către persoane neautorizate.
- 5) Mijloacele de prelucrare a datelor cu caracter personal, informația care conține 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 condițiile de licențiere.
- 7) Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

Secțiunea 2

Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal

22. Accesul în sediile/oficiile/birourile ori spațiile unde sînt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au permisiunea necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).

23. Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează 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, pereții exteriori ai încăperilor sînt rezistenți, intrările sunt echipate cu lacăte și semnalizare.

26. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

27. Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc persoanele desemnate.

28. Computerele, serverele, alte terminale de acces sînt 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, ținînd cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 al Legii nr.133 din 08.07.2011 privind protecția datelor cu caracter personal, precum și pct. 26 din Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale 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 prezenței unei permisiuni speciale a conducerii.

Secțiunea 3 Identificarea și autentificarea utilizatorilor și echipamentului. **Administrarea identificatorilor utilizatorilor**

31. Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.

32. Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conține semnamentele 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 și individuale ale persoanei.

34. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și 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 și autentificare se revocă sau se suspendă de administratorul TI.

35. Administrarea identificatorilor utilizatorilor include:

- 1) identificarea univocă a fiecărui utilizator;
- 2) verificarea autenticității fiecărui utilizator.

36. Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal, cu menținerea acestor informații pentru o perioadă îndelungată.

Secțiunea 4 **Utilizarea parolelor în procesul asigurării securității informaționale.** **Controlul administrării accesului**

37. La utilizarea parolelor sunt respectate regulile de asigurare a securității informaționale care prevăd:

- 1) păstrarea confidențialității parolelor;
- 2) interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;
- 3) modificarea parolelor de fiecare dată când 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 informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și 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 acțiunilor utilizatorilor se efectuează în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

Secțiunea 5 **Accesul de la distanță** **Limitarea folosirii tehnologiilor fără fir**

39. Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sînt documentate, supuse monitorizării și controlului.

40. Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este permisă de persoanele responsabile din cadrul [se indică localitatea] și permisă doar utilizatorilor, cărora aceasta le este necesară pentru îndeplinirea obiectivelor stabilite,

41. Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului.

42. Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.

43. Folosirea tehnologiilor fără fir se permite de persoanele responsabile din cadrul [se indică localitatea].

Secțiunea 6

Securitatea electroenergetică.

Controlul instalării și scoaterii componentelor TI

44. Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesanctionate, prin montarea lor în nișe speciale.

45. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

46. Sunt implementate sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sînt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

47. Este exercitat controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.

48. Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informație, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitîndu-se folosirea funcțiilor standarde de nimicire.

Secțiunea 7

Dezvăluirea datelor cu caracter personal

49. Dezvăluirea formatului electronic al datelor cu caracter personal conținute în sistemele de evidență, prin rețele comunicaționale ori pe alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN.

50. Accesul fără fir la sistemele de evidență a datelor cu caracter personal este permis doar utilizatorilor autorizați. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice asigurate de destinatar și operator, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți.

51. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere (expediere poștală cu aviz recomandat, înmînarea personală, etc.).

52. Este interzisă dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund Cerințelor (spre exemplu: expedierea informației 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 operațiunile de dezvăluire a datelor cu caracter personal între [se indică localitatea] și alte entități care sunt amplasate geografic în stînga Nistrului (regiunea transnistreană) care refuză să se supună juridic legislației Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii nr.133 din 08.07.2011 privind protecția datelor cu caracter personal.

54. Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecție 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 protecția datelor cu caracter personal, în special în cazurile cînd tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal.

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

57. Acces la datele cu caracter personal din sistemele informaționale gestionate în cadrul [se indică localitatea], din partea organelor de drept sau altor persoane se va permite doar în cazurile și condițiile prevăzute de legislația în vigoare.

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 adevărate circumstanțe care au importanță pentru cauză (inclusiv informația stocată în auditul sistemelor informaționale și de evidență), 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 și răspîndite fără necesitate informație oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație 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 instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

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 informație, datele cu caracter personal fac parte din categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

58. În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoștință cu fișa personală a clientului, aceștia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art.15 al Codului de procedură penală, art. 29 și art.30 al Legii nr.133 din 08.07.2011 privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art.741 al Codului Contravențional.

Secțiunea 8

Drepturile subiecților 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 protecția datelor cu caracter personal, acestuia i se furnizează următoarele informații, exceptînd cazul în care subiectul deține deja informațiile 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 evidență al operatorilor de date cu caracter personal);
- 2) privind scopul concret al prelucrării datelor cu caracter personal colectate;
- 3) privind destinatarul sau categoriile de destinatari ai datelor cu caracter personal;
- 4) dreptul la informare și de acces la datele colectate, de intervenție asupra datelor (în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația;
- 5) dreptul de acces și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neinclunderii sau inclunderii incorecte a unor date, precum și 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 alți subiecți, conținute în fișele personale (alte materiale), cu excepția cazurilor în care solicitantii își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.

61. Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entitățile ce asigură mentenanța sistemului și 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 intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaționale principale de stat etc.), modificarea urmînd a fi efectuată în toate sistemele informaționale și de evidență gestionate.

Secțiunea 9

Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate

63. Accesul în spațiile/perimetrul unde sînt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au permisiunea necesară conform politicii de securitate instituționale /regulamentelor departamentale aprobate.

64. Este interzisă stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității softului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului.

65. Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă.

66. Accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredințate 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 informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și 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.

Secțiunea 10

Auditul sistemelor informaționale gestionate

69. Înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem se efectuează conform următorilor parametri:

- a) data și timpul tentativei intrării/ieșirii;
- b) ID-ul utilizatorului;
- c) rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.

70. Înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, se efectuează conform următorilor parametri:

- a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
- b) denumirea (identificatorul) aplicației sau procesului, sau ID-ul utilizatorului;
- c) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
- d) tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
- e) rezultatul tentativei de obținere a accesului (executare a operațiunii) — pozitivă sau negativă.

71. Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

- a) data și timpul modificării competențelor;
- b) ID-ul administratorului care a efectuat modificările;
- c) ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

72. Înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces se efectuează conform următorilor parametri:

- a) data și timpul eliberării;
- b) denumirea informației și căile de acces la aceasta;
- c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
- d) ID-ul utilizatorului, care a solicitat informația.

Secțiunea 11

Asigurarea protecției contra programelor dăunătoare (virusurilor).

Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal

73. Protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal este asigurată prin existența programelor licențiate antivirus.

74. Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal (automat la pornirea sistemului și lunar la solicitarea utilizatorului autorizat în acest scop).

Secțiunea 12

Gestionarea incidentelor de securitate

75. Personalul/angajații [se indică localitatea] care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

76. Personalul/angajații [se indică localitatea] informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.

77. Prelucrarea incidentelor include: depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.

78. Până la data de 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrul Național pentru Protecția 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 și va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.

80. În cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar și va fi asigurat accesul la informațiile necesare relevante obiectului controlului.

Secțiunea 13

Marcarea documentelor.

Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată

81. Toată informația care se intenționează a fi dezvăluită, și care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.

Model: „Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr. 0000537-00X, înregistrat în Registrul de evidență al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal”.

82. Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 741 Cod contravențional) și penală (art. 177, art. 178, art. 180 Cod penal).

MODEL

Regulament privind prelucrarea datelor cu caracter personal în cadrul resursei informaționale în domeniul comerțului

I. Dispoziții generale

1. Regulamentul privind asigurarea securității datelor cu caracter personal din cadrul Sistemului informațional automatizat pentru gestionarea și eliberarea actelor permissive (în continuare - Regulament) este elaborat în vederea executării Legii nr. 133/2011 privind protecția datelor cu caracter personal, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123/2010, 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 permissive (în continuare – SIA GEAP) a fost creat în vederea executării prevederilor Hotărârii Guvernului nr.550/2018 Cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat de gestionare și eliberare a actelor permissive și Hotărârii Guvernului nr.551/2018 Pentru aprobarea Regulamentului cu privire la modul de ținere a Registrului actelor permissive [se va include prezenta hotărîre de Guvern după publicare].

3. Prezentul Regulament definește următoarele noțiuni:

date cu caracter personal - orice informație 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 identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

autentificare - verificarea identificadorului atribuit subiectului de acces, confirmarea autenticității;

identificare - atribuirea unui identificador subiecților și obiectelor de acces și/sau compararea identificadorului prezentat cu lista identificatoarelor atribuite;

integritate - certitudinea, necontradictorialitatea și actualitatea informației, care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;

mijloace de protecție criptografică a informației, care conține date cu caracter personal - mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației, care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acestora prin canalele de comunicații;

sesiune de lucru - perioada, care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și până la momentul opririi acestora;

utilizator - persoana, care acționează sub autoritatea deținătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal;

sistem informațional de date cu caracter personal – totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație, care conține 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. 231/2010 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 stabilește cerințele minime necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în procesul ținerii Registrului actelor permissive, care este format de către SIA GEAP, în conformitate cu prevederile Hotărârii Guvernului nr.550/2018 Cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat de gestionare și eliberare a actelor permissive.

5. În SIA GEAP datele cu caracter personal se prelucrează în scopul:

- 1) evidenței centralizate automatizate unice a actelor permissive eliberate de către autoritățile emitente indicate în Nomenclatorul actelor permissive eliberate de către autoritățile emitente persoanelor fizice și persoanelor juridice pentru practicarea activității de întreprinzător, aprobat prin anexa nr.1 la Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător și Legii nr. 231/2010 cu privire la comerțul interior;
- 2) înregistrării actelor permissive și asigurării consultării și obținerii extraselor din Registrul actelor permissive de către autoritățile publice, persoanele fizice și agenții economici din Republica Moldova;
- 3) asigurării formării resursei informaționale de stat privind actele permissive;
- 4) asigurării sistemelor informaționale departamentale cu date complete și veridice referitoare la actele permissive eliberate de autoritățile competente.

II. Categoria datelor cu caracter personal și 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 permissive aprobat prin Hotărârea Guvernului nr.551/2018, înregistrarea de stat a actelor permissive intră în atribuția autorităților emitente de acte permissive, iar ținerea Registrului de stat al actelor permissive 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 permissive, care se înscriu în Registrul actelor permissive, în conformitate cu prevederile Regulamentului cu privire la modul de ținere a Registrului actelor permissive aprobat prin Hotărârea Guvernului nr.551/2018.

8. În SIA GEAP se prelucrează datele cu caracter personal ale cetățenilor Republicii Moldova și cetățenilor străini solicitanți de acte permissive.

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 și/sau reședința;
- 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 și 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 permissive aprobat prin Hotărârea Guvernului nr.551/2018.

13. Utilizatorii în SIA GEAP sînt:

- 1) autoritatea emitentă de acte permissive – autoritatea publică centrală/locală care este implicată în eliberarea actelor permissive. Aceasta va procesa cererile și va înregistra în cadrul SIA GEAP datele privind actele permissive eliberate sau refuzate în conformitate cu prevederile Conceptului tehnic al Sistemului informațional automatizat pentru gestionarea și eliberarea actelor permissive 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 permise și care va completa formularele de cerere cu anexarea documentelor privind solicitarea actului permisiv, inclusiv cu eliberarea actului permisiv.

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

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

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

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

16. Agenția Servicii Publice este obligată să monitorizeze utilizarea datelor din Registrul actelor permise 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 securității, confidențialității și integrității datelor prelucrate în cadrul Registrului actelor permise se efectuează cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale, aprobate prin hotărâre de Guvern.

18. Regimul juridic de utilizare a datelor din Registrul actelor permise este stabilit în Capitolul IV din Regulamentul cu privire la modul de ținere a Registrului actelor permise aprobat prin Hotărârea Guvernului nr.551/2018.

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. 133/2011 privind protecția datelor cu caracter personal și legislația în vigoare.

20. Informarea subiectului se efectuează în conformitate cu Regulamentul cu privire la modul de examinare a adresărilor scrise ale cetățenilor și organizațiilor/instituțiilor în cadrul I.P. „Agenția 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 permise aprobat prin Hotărârea Guvernului nr.551/2018, datele recepționate din Registrul actelor permise nu pot fi transmise persoanelor terțe, dacă legislația în vigoare sau tratatele internaționale la care Republica Moldova este parte nu prevăd altfel.

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

22. Termenul prelucrării (păstrării) datelor cu caracter personal din SIA GEAP corespunde termenilor respectivi din reglementările aferente NIAC sau actelor permissive.

23. Datele de audit privind accesarea informației 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 funcționarea echipamentului tehnico-aplicativ și sistemelor informaționale 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 permissive sunt persoane cu funcție de răspundere, responsabile pentru colectarea, înregistrarea, organizarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea datelor cu caracter personal în Registrul actelor permissive, în limita competenței autorității emitente.

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

28. Administratorii pentru domeniile de competență din cadrul I.P. „Agenția Servicii Publice” și autorităților emitente de acte permissive de securitate sunt persoane cu funcție de răspundere, responsabile de securitatea și 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 GEAP).

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

29. Măsurile pentru asigurarea securității datelor cu caracter personal la prelucrarea acestora în SIA GEAP, se efectuează în conformitate cu Hotărârea Guvernului nr. 1123/2010 privind aprobarea cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, Conceptul tehnic al SIA GEAP aprobat prin Hotărârea Guvernului nr.550/2018, Regulamentul cu privire la modul de ținere a Registrului actelor permissive aprobat prin Hotărârea Guvernului nr.551/2018 și Politica de securitate a datelor cu caracter personal a I.P. „Agenția Servicii Publice”.

30. Modul de realizare a elementelor ciclului de viață a sistemelor software, precum și asigurarea funcționării mijloacelor tehnice și de program se efectuează în conformitate cu Regulamentul privind atribuțiile subdiviziunilor participante la administrarea resurselor informaționale ale I.P. „Agenția Servicii Publice”.

31. Gestionarea și configurarea funcțiilor de securitate a SIA GEAP se efectuează de către administratorul de sistem în conformitate cu Regulamentul privind atribuțiile subdiviziunilor participante la administrarea resurselor informaționale ale I.P. „Agenția Servicii Publice”.

32. Acordarea accesului utilizatorilor externi la SIA GEAP se efectuează în conformitate cu Regulamentul privind acordarea accesului la resursele informaționale deținute de I.P. „Agenția Servicii Publice” utilizatorilor interni și externi.

33. Informația recepționată din SIA GEAP se marchează în conformitate cu Cerințele de marcare a informației de ieșire ce conține date cu caracter personal în cadrul I.P. „Agenția Servicii Publice”.

34. Datele cu caracter personal din SIA GEAP sunt confidențiale. Acordarea informației din SIA GEAP se efectuează în conformitate cu Regulamentul privind acordarea accesului la resursele informaționale deținute de I.P. „Agenția Servicii Publice” utilizatorilor interni și externi.

35. Acordarea informațiilor 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 cetățenilor și organizațiilor/instituțiilor în cadrul I.P. „Agenția Servicii Publice” privind auditul operațiunilor de prelucrare a datelor cu caracter personal”.

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

37. Sunt supuse protecției toate resursele informaționale, care conțin date cu caracter personal, inclusiv:

- a) suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
- b) sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor, alte mijloace tehnice de prelucrare a informației.

38. Protecția datelor cu caracter personal prelucrate în sistemul informațional se efectuează prin următoarele metode:

- a) preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- b) excluderea accesului neautorizat la datele cu caracter personal prelucrate.

39. Preîntâmpinarea scurgerii de informații, care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, inclusiv cu utilizarea măsurilor organizaționale, tehnice și de regim.

40. Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea software-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității software-ului și efectuarea periodică a copiilor de siguranță.

XII. Securitatea mediului de funcționare

41. Securitatea mediului de funcționare reprezintă protecția fizică a resurselor informaționale de accesul nesancționat, deteriorări și perturbații, adică amplasarea lor în încăperi securizate, delimitate de un anumit perimetru al securității.

42. Accesul în spațiile securizate, unde sunt amplasate serverele este restricționat, fiind permis doar persoanelor, care au autorizația necesară, în timpul orelor de program, doar în caz de necesitate și se interzice aflarea persoanelor terțe.

43. În scopul asigurării securității utilajului, acesta este amplasat într-o încăpere aparte la loc vizibil, amenajată cu climatizator puternic, în cutii de metal, minimalizând acțiunile pericolelor obișnuite, artificiale, tehnogene și naturale.

XIII. Gestionarea incidentelor de securitate din cadrul SIA GEAP

44. Utilizatorii datelor Registrului actelor permissive, în procesul conectării la sistem, în mod obligatoriu, vor trece instruirea de reacționare la incidentele de securitate informațională contra semnătură.

45. Utilizatorii și administratorii utilizatorilor datelor Registrului actelor permissive, în cazul apariției incidentelor legate de încălcarea securității, sunt obligați să informeze neîntârziat subdiviziunea responsabilă din cadrul I.P. „Agenția Servicii Publice”.

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

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

SINTEZA
Obiecțiilor și propunerilor (recomandărilor)
la proiectul hotărârii Guvernului „Cu privire la instituirea resursei informaționale în domeniul comerțului”
Nr. 92/MEI/2018

Participantul la avizare (expertizare)/ consultare publică	Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
1. Agenția de Guvernare Electronică <i>(demersul nr. 3007-76 din 01.11.2018)</i>		
	1. Modificare în text a denumirilor platformelor și serviciilor electronice guvernamentale.	1. Se acceptă.
	2. Reformularea la pct. 9, noul subpunct 14 literele a) și b).	2. Se acceptă.
	3. Modificarea literei l) la pct. 9, noul subpunct 14.	3. Nu se acceptă , dat fiind faptul că refuzul urmează a fi unul motivat, fiind și motiv pentru contestare. Termenii de prescripție în acest sens putând fi modificați prin cadrul normativ care nu este nemijlocit legat de SIAGEAP.
	4. Reformularea gramaticală a noului subpunct 18, litera a).	4. Se acceptă.
2. Agenția Servicii Publice <i>(demersul nr. 01/6397 din 01.11.2018)</i>		
	1. În opinia autorilor avizului prin PHG NIAC i se conferă statut de act permisiv fapt ”ideologic” incorect.	În scopul examinării propunerilor și obiecțiilor expuse în avizul, pe data de 09.11.2018 în incinta MEI, a fost organizată o ședință în care căreia unele aspecte au fost elucidate și scoase de pe rol (Procesul-verbal se anexează), printre care: 1. S-a explicat statutul NIAC, sarcinile Guvernului în acest sens

		și condițiile care au dus la decizia utilizării SIAGEAP ca platformă pentru resursa informațională în comerț. Prin proiectul de hotărîre a Guvernului propus, NIAC nu i se conferă statut de act permisiv dat fiind faptul că aceasta este imposibil de a realiza printr-o hotărîre de Guvern. Toate actele permissive sunt cuprinse exhaustiv în anexa la Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător. MEI este dezvoltatorul și promotorul principal al reformei cadrului de reglementare a activității de întreprinzător care a dus la reducerea numărului de acte permissive cu 264. Prin adoptarea proiectului de hotărîre în cauză se conferă formă juridică unui fapt împlinit. În SIAGEAP deja este inclusă și testată funcționalitatea NIAC. Utilizarea platformei SIAGEAP pentru realizarea sarcinii legale de instituire a resursei informaționale în domeniul comerțului (RIC) este dictată de motive practice. Prin utilizarea SIAGEAP se economisesc timp și mijloace bugetare, care au fost alocate deja pentru dezvoltarea sistemului în complex pentru 152 de acte permissive. Suplimentar, NIAC prevede și posibilitatea solicitării prin interoperabilitate a informațiilor din alte surse de TI, întru evitarea prezentării de acte inutile, precum ar fi extrasul din Registrul persoanelor juridice, precum și solicitarea/verificarea unor acte permissive, fapt care este lesne de hotărât în interiorul unui singur sistem de TI. Adoptarea proiectului de hotărîre a Guvernului va permite crearea și gestionarea resursei informaționale în domeniul comerțului de către Guvern, fapt care se încadrează perfect în prevederile legale, și nu comportă nici un aspect ”ideologic”.
	2. Legea nr. 231/2010 art. 4 lit. d) stabilește sarcina pentru MEI - ”<i>monitorizarea activităților de comerț (crearea și gestionarea resursei informaționale în domeniul comerțului)</i>”.	2. Autorii susțin corect că, MEI în calitatea de exponent al Guvernului urmează să creeze și gestioneze resursa informațională în domeniul comerțului (RIC). În acest sens, evidențiem că nu există careva contradicții. Prin adoptarea proiectului de hotărîre a Guvernului se va realiza

		cerința legală. Art. 3 din Legea nr. 231/2010 prevede că resursă informațională de stat este creată și administrată de Guvern, care conține date privind unitățile comerciale și locurile de vânzare și permite interacțiunea autorităților administrației publice locale cu alte resurse informaționale de stat și autorități publice în privința relațiilor ce țin de comerțul interior”.
	3. Proiectul de hotărîre a Guvernului ”<i>nu va soluționa integral cerințele Legii 321/2010</i>”.	3. Nu se acceptă. A se vedea argumentele de la pct. 2 de mai sus.
	4. ASP propune ”<i>implementarea NIAC în Registrul actelor locale</i>”.	4. Nu se acceptă. A se vedea argumentele de la pct. 1 și pct. 2 de mai sus. Suplimentar, atenționăm că ”<i>implementarea</i>” presupune inițial selectarea companiei dezvoltatoare, bugetarea, coordonarea cu autoritățile și testarea. Toate acestea ar însemna o risipă de timp și bani. Legea nr. 153/2016 pentru modificarea și completarea unor acte legislative prevede în alin. (2) art. X expres termenul 12 luni în care Guvernul va asigura crearea, funcționarea și întreținerea resursei informaționale în domeniul comerțului - termen deja expirat. Utilizarea platformei ”Registrului actelor locale” în opinia noastră este irelevantă din motivul că acesta conține actele normative emise de către autoritățile administrație publice locale (APL) unde ar trebui să se conțină spre exemplu Regulamentul privind comerțul în localitate aprobat printr-o decizie a Consiliului local. În cazul NIAC se prevede o procedură distinctă reglementată de norme juridice cu caracter special la nivel de lege, prin care legiuitorul a decis investirea APL cu atribuții speciale în domeniul comerțului. Prin urmare, procedura NIAC este una stabilită prin lege, iar procedura de operare cu NIAC este decisă de Guvern, dar NIAC nu constituie un act emis de APL ci recepționat și verificat. Pentru argumentarea soluției de ”<i>implementare a NIAC în</i>

		<i>Registrul actelor locale</i>” autorii avizului ar trebui să vină cu o analiză argumentată privind eficiența unei astfel de soluții, în special, din perspectiva faptului că NIAC în SIAGEAP este o funcționalitate deja existentă, dezvoltată, testată și acoperită financiar. Un alt subiect ce urmează a fi elucidat este relația dintre deținătorii sistemelor prin asigurarea interoperabilității de care este responsabilă Agenția de Guvernare Electronică. În cazul Registrului actelor locale responsabil de politici este Cancelaria de Stat iar administratorul tehnic este Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”. În cazul SIAGEAP posesor este MEI iar deținător (tehnic) ASP. Prin urmare, soluția propusă de APL va genera probleme de ordin birocratic și tehnic implicând cel puțin 5 autorități cu atribuții similare pentru o singură resursă informațională. Nu vedem NIAC în afara SIAGEAP și din perspectiva posibilității solicitării prin intermediul ghișei unic asigurat de SIA GEAP acte permissive lipsă aferente NIAC, de exemplu în cazul autorizații sanitare și sanitar-veterinare. Aici SIAGEAP oferă posibilitatea solicitării în cadrul aceluiasi sistem a acestora fără necesitatea logării în alte sisteme sau obținerii acestora în baza vizitei fizice la autorități, fapt care simplifică radical procesul de lucru în sistem și reduce timpul de începere al activității de comerț cel puțin cu perioada obținerii preventive a acestor acte suplimentare. Din această perspectivă ASP va fi oricum implicat în procesul eliberării NIAC prin deservirea situației de mai sus chiar dacă se va ajunge la setarea NIAC în alt sistem. Suplimentar, atenționăm că în proiectul hotărîrii Guvernului propus ASP este exceptat de funcția de front-office pentru depunerea NIAC, acest rol revenind în exclusivitate APL. Prin urmare, ASP va exercita funcțiile de deținător al SIAGEAP în
--	--	---

		același sens pe care îl are pentru actele permissive. Registrul actelor locale nu prevede în calitate de actori persoane (fizice și juridice) neoficiale, care ar putea introduce date în sistem. Funcționalități care urmează a fi dezvoltate suplimentar dacă se va decide. Deci, Registrul actelor locale este unul de tip închis. Cu un nivel de securitate necesar inferior celui pentru SIAGEAP. Schimbarea situației ar implica modificări esențiale în Hotărîrea Guvernului nr.672/2017 pentru aprobarea regulamentelor cu privire la Registrul de stat al actelor locale și modificarea contractelor de mentenanță cu Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, ce poate genera cheltuieli bugetare suplimentare. În concluzie, reliefăm că schimbarea platformei va necesita modificări legislative importante, cel puțin la Legea nr.231/2010 și la Hotărîrea Guvernului nr. 672/2017.
3. Agenția Națională pentru Sănătate Publică <i>(demersul nr. 01/3429 din 02.11.2018)</i>		
	Fără obiecții	
4. Cancelaria de Stat a Republicii Moldova <i>(demersul nr. 21-06-9016 din 08.11.2018)</i>		
	1. Excluderea din preambul a referinței la Hotărâri de Guvern. 2. Excluderea din preambul a referinței la Legea nr. 153/2016. 3. Modificarea pct. 5 din proiectul hotărîrii Guvernului prin excluderea sintagmei ”Cancelaria de Stat”.	1. Se acceptă. 2. Se acceptă. 3. Se acceptă parțial , sintagma se va modifica în: ”Ministerul Economiei și Infrastructurii de comun cu.....”, dat fiind faptul că doar Cancelaria de Stat are dreptul să verifice legalitatea actelor

		emise de APL și să intervină atunci când se constată o ilegalitate sau există o parte vătămată, conform Legii nr. 436/2006 privind administrația publică locală.
5. Centrul Național Anticorupție <i>(demersul nr.06/2-6405 din.08.11.2018)</i>		
	III. Concluzia expertizei	
	1. Modificarea referinței la art. 15 și 212 al Codului de procedură penală, din Capitolul 7, pct. 57 al modelului de Politica de securitate a datelor cu caracter personal în cadrul [se indică localitatea], fiind considerate drept unele care îngustează accesul la informații relevante unor organe de drept, instanțelor de judecată etc.	Se acceptă. Se propune următoare redacție. ”57. Acces la sistemele informaționale gestionate în cadrul [se indică localitatea], din partea organelor de drept, sau altor persoane va fi permis doar în cazurile și forma prevăzute de lege”.
6. Ministerul Justiției <i>(demersul nr.04/12511 din 01.11.2018)</i>		
	La proiectul hotărârii Guvernului:	
	1. Modificarea denumirii actului normativ.	1. Se acceptă.
	2. Modificarea clauzei.	2. Se acceptă.
	3. Excluderea modelelor.	3. Nu se acceptă. Propunem să fie păstrate din motive practice. Ca exemplu, modelul Regulamentului de comerț în localitate a fost plasat pe pagina web a MEI cu mult înainte, au fost emise scrisori informative privind respectarea reglementărilor legale în acest sens (Legile nr.231/2010 și nr.153/2016). Însă, până în prezent există reticențe la acest capitol. Considerăm că includerea acestora în textul proiectului hotărârii Guvernului va da un impuls repetat, inclusiv de ordin practic pentru conformarea APL-urilor cerinței legale.

		În cazul anexelor aferente actelor necesare înregistrării la CNPDCP raționamente de includere a modelelor au fost unele practice. Au fost situații în care autoritățile emitente nu cunoșteau procedura (actele ce urmează a fi elaborate) și solicitau suport inclusiv practic pentru a fi înregistrate în calitate de operator al datelor cu caracter personal. Păstrarea acestora nu poate genera ambiguități, dat fiind faptul că este stipulat expres că acestea sunt modele. Totodată, în lumina proiectului de lege pentru modificarea și completarea unor acte legislative prin care se propune modificarea Legii nr.133/2011 privind protecția datelor cu caracter personal, urmare a abrogării Directivei 95/46/CE și racordării Legii nr.133/2011 la Regulamentul (UE) nr. 2016/679, pentru modificarea procedurii de înregistrare la CNPDCP cu aderarea instituțiilor publice la un corp de reguli. Însă, proiectul dat se află doar la etapa avizării și este puțin probabil ca acesta să fie aprobat în Parlamentul Republicii Moldova în sesiunea curentă, sau chiar soarta proiectului în general, pe când pentru proiectul în discuție urmează să fie măsurile ce se impun de cadrul normativ în vigoare.
	4. Revizuirea pct. 2 prin prisma art. 7 al Legii nr. 161/2011.	4. Se acceptă parțial. Nu se instituie un SI nou ci se completează Conceptul SIAGEAP unde sunt prevăzute rolurile autorităților în sistem. Legile nr.231/2010 și 153/2016 pun în sarcina Guvernului dezvoltarea în anumiți termeni și gestionarea resursei informaționale în domeniul comerțului. Ca exponent al guvernării, MEI este autoritatea centrală care coordonează procesul cu alte autorități centrale și autoritățile administrației publice locale (art. 5 alin. 2, Legea nr.231/2010).
	5. Excluderea pct. 4 din proiectul hotărârii Guvernului.	5. Nu se acceptă. A se vedea argumentele de la pct. 3. Suplimentar, este adevărat că APL-urile aveau obligația și

		termeni de a adopta Regulamentele, stabilită de Legea nr.153/2016, însă acestea nu s-au conformat. MEI nu are pârghii legale ce ar influența APL, conlucrarea cu acestea fiind de competența Cancelariei de Stat, aceasta fiind și argument pentru a păstra Cancelariei de Stat în pct. 6 al proiectului hotărârii Guvernului (A se vedea pct. 6 de mai jos).
	6. Revizuirea pct. 5 din textul HG.	6. Se acceptă parțial. Se propune de a modifica conținutul în următoarea redacție: ”Ministerul Economiei și Infrastructurii de comun cu.....”, dat fiind faptul că doar Cancelaria de Stat are dreptul să verifice legalitatea actelor emise de APL și să intervină atunci când se constată o ilegalitate sau există o parte vătămată, conform Legii nr. 436/2006 privind administrația publică locală.
	7. Reformularea pct. 6 din textul HG.	7. Se acceptă. Termenii diversificați de intrare în vigoare sunt dictați de complexitatea procesului de implementare. Sunt peste 900 de APL de ambele niveluri cu dotări de personal și tehnică diferită, iar PHG presupune anumite acțiuni preparatorii pentru care este necesar de timp. Similară este și situația cu autoritățile centrale, existînd necesitatea implementării în reprezentanțele teritoriale. În ambele situații se vor efectua vizite informative și de instruire în teritoriu. Excluderea acestui termen de conformare cerințelor incluse în PHG va compromite implementarea practică a resursei informaționale în comerț.
	La Anexe:	
	1. Art. 17 ⁹ presupune că prin intermediul resursei informaționale în domeniul comerțului, instituită și administrată de Guvern se duce evidența și monitorizarea unităților comerciale și a locurilor de vânzare, precum și a datelor aferente acestora.	1. Se acceptă. Nu sunt contradicții dintre proiectul hotărârii Guvernului și prevederea legală, dat fiind faptul că NIAC se depune pentru fiecare unitate comercială și loc de vânzare, evidența este asigurată prin emiterea unui număr unic pe țară, iar monitorizarea este

		asigurată prin evidența modificărilor sau încetărilor de NIAC la nivel național. Suplimentar, SIAGEAP este un sistem deschis care poate fi modificat urmare a modificărilor cadrului normativ prin includerea oricăror funcționalități suplimentare necesare. Conceptele propuse spre modificare nu constituie instrucțiuni de utilizare ci arată conceptual organizarea și funcționarea sistemului. Arhitectura sistemului este setată în baza cadrului legal și prin conlucrare cu autoritățile prin emiterea și aprobarea pașaportului aferent fiecărei funcționalități, unde drept finalitate este semnarea UAT (user acceptance test) de către dezvoltator și autoritate. O astfel de abordare permite flexibilitatea sistemului și introducerea de modificări rapide în acesta urmare a modificării cadrului de reglementare sau necesității suplinirii cu alte obiecte informaționale.
	2. Corectări redacționale.	2. Se acceptă. Au fost efectuate modificările respective.
	3. Excluderea noțiunilor aferente NIAC și APL.	3. Nu se acceptă. APL-urile și ASP pe parcursul ședințelor privitor la examinarea proiectului hotărârii Guvernului au insistat asupra separării foarte clare a obiectelor informaționale și noțiunilor aferente în textul proiectului hotărârii Guvernului, precum și a numirii în clar a autorităților implicate de operare în SIAGEAP. Păstrarea acestora corespunde scopului proiectului hotărârii Guvernului și logicii constituirii unui SI, pe când excluderea ar putea afecta avizarea ulterioară din partea instituțiilor menționate supra. APL fiind principalul operator în sistem al NIAC iar ASP fiind deținătorul de sistem, au propriile cerințe față de descrierea funcționalităților și noțiunilor respective.
	4. NIAC contravine sensului expus în Legea nr. 231/2010,... notificarea ... se încadrează în categoria actelor permissive.	4. Nu se acceptă. Prin proiectul hotărârii Guvernului propus NIAC nu i se conferă statut de act permisiv, dat fiind faptul că aceasta este imposibil de realizat printr-o hotărâre de Guvern. Toate actele permissive sunt

		cuprinse exhaustiv în anexa la Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător. MEI este dezvoltatorul și promotorul principal al reformei cadrului de reglementare care a dus la reducerea numărului de acte permise cu 264. Pentru economisirea de resurse financiare și timp pentru NIAC este utilizată platforma informațională dezvoltată pentru actele permise. Platforma comună (SIAGEAP) nu înseamnă și statut identic. Statutul actului permisiv este stabilit prin lege. Pentru a exclude contradicțiile la acest subiect se propune a introduce modificări și în textul Hotărârii Guvernului nr.753/2016. (A se vedea redacția revizuită).
	5. Evitarea confuziei privind eliberarea NIAC de către APL.	5. Se acceptă. Se suplinește pct. 14) litera h) la modificările din Concept.
	6. Evitarea tautologiei juridice la pct. 5.	6. Se acceptă A fost exclusă sintagma ” <i>inclusiv autoritățile administrației publice locale</i> ”.
	7. Privind revizuirea din pct.9.	7. Nu se acceptă. Pct. 29 din Concept inițial conține 13 subpuncte fiind completate subsecvent.
	8. Revizuirea pct. 57 din anexa nr. 3.	8. Se acceptă. Se propune următoarea redacție: ”Acces la datele cu caracter personal din sistemele informaționale gestionate în cadrul [se indică localitatea], din partea organelor de drept sau altor persoane se va permite doar în cazurile și condițiile prevăzute de legislația în vigoare”.
	9. Excluderea Capitolului XIV la anexa nr. 4	9. Se acceptă.
7. Centrul Național pentru Protecția Datelor cu Caracter Personal <u>(demersul nr.04-06/2386)</u>		

din 12.11.2018)		
	1. Actul normativ are caracter public și obligatoriu opozabil tuturor subiecților de drept vizați, se consideră irelevantă utilizarea sintagmelor ”se propune” și ”se recomandă”.	1. Nu se acceptă. Obligația legală fiind deja existentă, Guvernul, respectînd principiul autonomiei locale, reiterează necesitatea conformării.
	2. La anexa nr.3 - modificări redacționale.	2. Se acceptă.
	3. La anexa nr.4 - modificări redacționale	3. Se acceptă.
8. Congresul autorităților publice locale <i>(demersul nr.98 din 22.10.2018)</i>		
	Avizul a fost întocmit la proiectul de hotărîre înainte de avizarea oficială. Pe data de 23.10.2018 în incinta MEI a fost organizată o ședință, în cadrul căreia a fost luat act de unele observații și propuneri fiind ulterior incluse în textul proiectului remis spre avizare.	
	Per general CALM presupune că ”se încearcă de a utiliza același mod de implementare a soluțiilor tehnice ca în sectorul privat (de afaceri), lucru absolut inadmisibil în sectorul public, unde primordial nu este randamentul sau eficiența economică, dar asigurarea interesului public și proporționalitatea dintre interesul public și privat”.	Considerăm că, economia de resurse pentru mediul de afaceri pentru înregistrarea afacerii este evident în interesul APL, prin prisma atragerii businessului într-o localitate concretă cu defalcările ulterioare implicate în bugetul local. Guvernul, executând prevederile legale, a dezvoltat din resursele proprii și pune la dispoziția APL un instrument contemporan de evidență și gestionare a notificărilor privind inițierea activității de comerț. Acces la datele din sistemul electronic APL îl vor avea instantaneu. Utilizarea sistemului de TI nu împiedică APL să păstreze copiile pe hârtie ale actelor aferente Notificării și

		Notificarea propriu-zisă. În acest sens, Legea nr. 231/2010 prevede la alin. (5) al art. 15 că <i>notificările și copiile actelor anexate, depuse de comerciant, se păstrează în arhiva autorității administrației publice locale.</i> Prin proiectul de hotărâre nu se impun sarcini noi pentru APL, ci doar se propune schimbarea formei de evidență. Actualmente, orice APL are desemnate persoane care recepționează Notificările pe suport de hârtie, urmat de o înregistrare în evidențele proprii (oricare ar fi ele, pe hârtie sau de TI). Prin urmare, aceiași persoană (funcționar public) se va putea loga în sistemul SIAGEAP pentru a înregistra o Notificare. Menționăm că, toți funcționarii publici posedă semnătură electronică. De aici derivă excluderea necesității de creare a unui nou post de lucru. Păstrarea informației generale pe țară privind Notificările la fel nu poate afecta autonomia locală, serviciile electronice guvernamentale bucurându-se de nivelul de protecție a datelor cerut de lege, iarăși din surse guvernamentale, pe care APL nu le vor putea acoperi tehnic și financiar, MEI avînd obligațiuni stipulate expres în acest sens în literele e) și g) ale art. 5 din Legea nr. 231/2010: - ”<i>coordonarea activităților organelor centrale de specialitate ale administrației publice și ale autorităților administrației publice locale în domeniul comerțului interior</i>”, - ”<i>monitorizează, prin intermediul resursei informaționale în domeniul comerțului, activitatea de comerț desfășurată pe teritoriul localității respective</i>”.
9. Primăria mun. Chișinău (demersul nr.02-106/7005 din 05.11.2018)		
	Susține proiectul cu unele propuneri redacționale	
	1. Înlocuirea termenului „ <i>eliberare</i> ,” cu	1. Se acceptă.

	"recepționare" cu referire la NIAC din pct. 6 ¹ și 6 ³ .	Pentru pct. 6 ¹ , pentru 6 ³ se modifică în termenul "gestionare".
	2. Introducerea sintagmei "recepționară" în noțiunea de NIAC.	2. Se acceptă.
	3. Excluderea sintagmei "permissive" din pct.3 (subpct. 8 al pct. 12 din Concept).	3. Se acceptă.
	4. Excluderea NIAC din lista documentelor de ieșire, pct. 6.	4. Nu se acceptă , dat fiind faptul ca sintagma "documente de ieșire" din Concept este una generică pentru actele pe care le generează SIAGEAP. Aici nu se schimbă statutul NIAC ci doar se stabilesc proceduri tehnice de operare cu obiectele unui sistem de TI. Statutului actului NIAC este stabilit prin Legea nr. 231/2010.
	5. Suplinirea pct. 15 din Concept prin introducerea referinței la Legile nr. 231/2010 și nr.153/2016.	5. Se acceptă.
10. Agenția Națională pentru Siguranța Alimentelor <u>(demersul nr.01-6/3325 din 05.11.2018)</u>		
	1. Suplinirea Capitolului I al Regulamentului de desfășurare a activității de comerț în localitate.	1. Nu se acceptă , dat fiind faptul că această prevedere ține de competența APL și trebuie să se încadreze în limitele admise de art. 6 din Legea nr. 231/2010.
	2. Alte sugestii redacționale.	2. Se acceptă.