MINISTERUL EDUCAŢIEI,CULTURII ŞI CERCETĂRII AL REPUBLICII MOLDOVA

UNIVERSITATEA DE STAT DE EDUCAȚIE FIZICĂ ŞI SPORT

CATEDRA PROTECȚIE, PAZĂ ȘI SECURITATE

Andrei Nastas Irina Antoșciuc Nicolae Corcea

GHID METODIC

„REGIMUL NORMATIV AL INFORMAȚIEI”
(aspecte normativo-juridice)

CHIȘINĂU 2020

Lucrarea este recomandată spre publicare de Senatul USEFS (proces-verbal nr.1, din 01 octombrie 2020).

Recenzenţi:

Radion COJOCARU, doctor în drept, conferențiar universitar

Sergiu CERNOMOREȚ, doctor în drept, conferențiar universitar

Corectura: Natalia CIOBANU, master în filologie, doctorandă

Redactare tehnică, procesare computerizată: ***Valeriu EFREMOV***

Descrierea CIP a Camerei Cărții Naționle

Nastas, A ndrei

Ghid metodic „Regimul normativ al informației"(aspecte normativo-juridice)/ Andrei Nastas, Irina Antoșciuc, Nicolae Corcea. Ministerul Educaşiei, Culturii şi Cercetării al Republicii Moldova.Universitatea de Stat de Educației Fizică și Sport. Catedra Protecție, Pază și Securitate.- Chișinău: Iulian, 2020 (Tipogr. „Cetatea de Sus")- 460 p.: fig.,tab.

Bibliogr.: p. 455-460. - 100 ex.

ISBN 978-9975-3393-2-2 342.72/.73(075)

N 24

Ghidul metodic a fost elaborat în conformitate cu curricula cursului „Regimul normativ al informației" din cadrul Facultății PPS a universității. Prezenta lucrare este recomandată tuturor studenților, în mod deosebit, celor care fac studiile la Ciclul I ăn cadrul USEFS, inclusiv cadrelor didactice din alte instituții de învățământ din țară.

CUPRINS

Introducere

Din momentul în care a apărut omenirea,informația despre lumea înconjurătoare reprezenta o resursă destul de importantă,cu referire la supraviețuirea acest*eia și activitățile ulterioare.* În procesul său de evoluție,omenirea nu numai că a acă*parat un volum enorm de informație,dar și a învățat să coopereze cu aceasta sub diferite forme. Lumea modernă - este lumea informației,cea care joacă un rol extrem de important în procesul de evoluție al omenirii,* în economie, în învățământ, în educație, în drept și multe alte sfere la fel de importante al dezvoltării statului și al*e societății. O perioadă lungă de timp, nimeni nu a contribuit la dezvoltarea întrebărilor asupra importanței informației, și doar în secolul XX au apărut și au a evoluat activ prevederile legale, care reglementează relațiile relevante în domeniul informativ.*

În ziua de astăzi putem vorbi despre *formarea unei noi ramuri de drept „Dreptul informațional",care se află chiar la început de cale. Cu atât mai mult că astăzi există deja o necesitate activă a unui regulament juridic al relațiilor informaționale.*

*Scopul acestui ghid este regulament de o analiz*ă a *cadrul legislativ a Republicii Moldova în cadrul diferitelor tipuri de informații.*

*Această analiză juridico-normativă va fi util*ă *studenților și masteranzilor la învățarea disciplinelor relevante, juriștilor și altor practicanți care sunt subiec*ți *de informații juridice, oamenilor de știință care explorează o nouă legislație cu referire la dreptul de informare și informație*

Conceptul informativ, indicii şi tipurile acesteia

În ziua de astăzi în Republica Moldova lipseşte *orice tip de regulament, care ar stabili o dispoziție generală despre informație,* în ar fi explicat conceptul informativ, *indiciile și categoriile sale, metodele de formare ale acesteia, schimbările sau chiar distrugerea informației .*

Din păcate,legislația statului a luat o reflecție mai amplă asupra diferitor legi privind distribuirea informației utilizate anume în anumite contexte ale legii, ce face înțelegerea informației din punct de vedere obiectiv nesistemică.

Aşadar,în conformitate cu articolul 37 al Codului cu privire la ştiinţă şi inovare:[1]*,, Informaţie ştiinţifico-tehnologică este informaţia care reflectă rezultatele activităţii din domeniile cercetării şi inovării din ţară şi străinătate"*

Cu referire la art. 6 al legii ,,privind accesul la informaţie."[2]*: ,,informaţii oficiale sînt considerate toate informaţiile aflate în posesia şi la dispoziţia furnizorilor de informaţii, care au fost elaborate, selectate, prelucrate, sistematizate şi/sau adoptate de organe ori persoane oficiale sau puse la dispoziţia lor în condiţiile legii de către alţi subiecţi de drept. "*

Legea ,,Cu privire la Sistemul informaţional integral automatizat de evidenţă a infracţiunilor, acauzelor penale şi a persoanelor care au săvîrşit infracţiuni[3] *introduce noțiunea de informație de ordin criminal și în articolul 2 al Codului Penal i se conferă următoarea definiție ,,i*nformaţie cu caracter criminal – *informaţie despre infracţiunile înregistrate şi persoanele care le-au săvîrşit, despre alte categorii de persoane luate la evidenţa centralizată specială în conformitate cu prezenta lege, despre obiectele marcate şi obiectele de anticariat, alte date ce caracterizează infracţiunile şi circumstanţele comiterii lor."*

Conform art. 3 din Legea,,cu privire la informatizare şi la resursele informaţionale de stat"[4]*, i*nformaţia reprezintă *cunoştinţe despre persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situaţii şi idei.*

---

[1] COD Nr. 259 din 15.07.2004 cu privire la ştiinţă şi inovare al Republicii Moldova Publicat : 30.07.2004 în Monitorul Oficial Nr. 125-129

[2] LEGE Nr. 982 din 11.05.2000 privind accesul la informaţie Publicat : 28.07.2000 în Monitorul Oficial Nr. 88-90

[3] LEGE Nr. 216 din 29.05.2003 cu privire la Sistemul informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni Publicat : 08.08.2003 în Monitorul Oficial Nr. 170-172

[4] LEGE Nr. 467 din 21.11.2003 cu privire la informatizare şi la resursele informaţionale de stat Publicat : 01.01.2004 în Monitorul Oficial Nr. 6-12

În același timp,această definiție nu se aplică,*luând în considerare art.1,p.2 al Legii,cu referire la relațiile,care apare în timpul creării și funcționării resurselor informaționale în masă,precum și din prelucrarea informației nedocumentare.*

După cum observăm,lipsa unui singur act,elaborat cu o reglementare

juridică care ar conține în sine o definire a informației, ca rezultat într-un fel juridic,ale cărei încercări de umplere se face prin introducerea unei serii de informații de diferite tipuri nu există astfel apar mai multe dificultăți. Această distorsiune a sensului de informații, dând caracteristici extriseci sau invers-îngustează sensului noțiunii de informație. În legătură cu aceasta,sub termenul de informație este acceptabil să înțelegem următoarele:

*Informația (prov. de la lat. Informatio – „lămurire,*închipuire,înțelegere",- de la lat. Informare- „a da formă,a învăța,a gândi,a închipui"*) - informația indiferent de forma sa de prezentare, percepută de către o persoană sau un dispozitiv special, este o reflectare a lumii materiale, a faptelor în procesul de comunicare.*

Definirea noțiunii de „informație" din standarde internaționale:

- ✓ *Cunoștințe despre obiecte,fapte,idei,etc.,de care oamenii pot face schimb în anumite contexte (ISO/IEC 10746-2:1996);*
- ✓ *Cunoașterea faptelor,evenimentelor,lururilor,ideilor și conceptelor,care într-un anumit context au o anumită semnificație (ISO/IEC 2382:2015);*

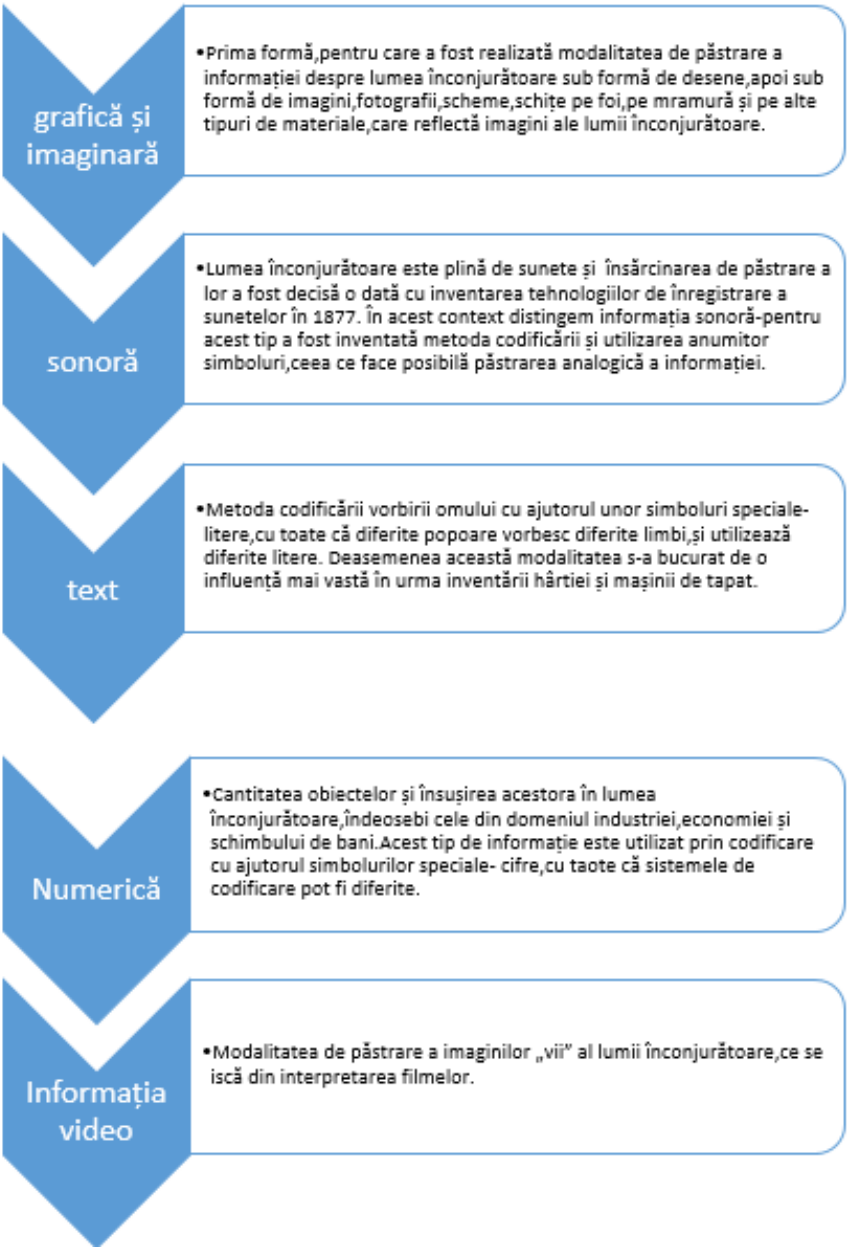
Generalizând termenul de „informație"se înțelege transmiterea unui text oamenilor în formă orală,scrisă sau oricare altă formă existentă (cu ajutorul diferitelor semne sau tehnologii etc.).

Din mijlocul sec. XX, termenul de „informație" s-a transformat într-o înțelegere științifică,care include în sine schimbul de informație dintre oameni, **între un om și un robot** *,între roboți, schimbul de semne cu animalele și cu lumea în dezvoltare, transmiterea semnelor de la o celulă la alta, de la un organism la altul (de exemplu,informația genetică),una din esențialele înțelegeri ale ciberneticii.*

Indicii de bază ai informației

Informația este în continuă evoluție	•Aceasta este replicată,însă nu se pierde,poate fi distribuită într-o cantitate extrem de vastă a exemplarelor practic fără a fi schimbată în ceea ce privește conținutul acesteea și fără a-și pierde calitatea.Poate aparține mai multor persoane și utilizată de nenumărate ori fără a pierde volumul și calitatea ulterioară.
Bi-unitatea informației și deținătorul ei	•Informația de regulă are și un deținător al său.Informația este transmisă și distribuită în majoritatea cazurilor,purtătorilor de informații și cu ajutorul purtătorului de informație.
Caracterul fizic și inalienabil al informației	•În momentul transmiterii sau producerii informației,ea nu trece de la un subiect la altul,fiind capabilă de a fi transmisă de nenumărate ori.Astfel,alienabil devine numai purtătorul de informație cu informația propriu-zisă.
Informația nu are o localizare anume în univers	•De regulă este localizat doar purtătorul de informație.Informația poate fi transmisă ușor cu ajutorul tehnologiilor moderne de comunicație,poate fi transmisă la distanțe destul de mari fără a-și pierde din calitate.
Omul ca consumator principal	•Unul din principalii consumatori al informațiilor este omul,care este capabil nu doar să primească informația sub diferite forme,dar și să o păstreze,să o producă în diverse moduri,precum și să sistematizeze o nouă informație în rezultatul unei gândiri asupra anumitor fapte.
De regulă informația prevede o formă organizatorică	•Aceasta are o structură la fel ca și un sistem de informare,documente,bibliotecă etc.Pentru subiecții informației trecuți prin procesul de sistematizarea a acesteea,analizează și adaugă informația de care dispun ei înșăși.
Informația poate fi măsurată în cantitate	•În acest context pot fi utilizate așa valori precum sunt cantitățile de simboluri,semne...
Informația are o valoare deosebită	•Valoarea informației poate fi apreciată în bani.Cu toate acestea nu există modalități anume de a pune preț informației,deoarece valoarea acesteea poate diferenția decisiv în conformitate cu o mulțime de factori.

Tipurile informației



Proprietățile calitative ale informației:

Din punctul de vedere al informaticii,cele mai importante proprietăți calitative ale informației sunt:

*Obiectivitatea,precizia,integritatea,exactitatea,actualitatea,utilitatea,valoarea,*înțelegerea*,accesibilitatea,concizia.*

***1.Obiectivitatea informațiilor**. Obiectiv - existent în afara și independent de conștiința umană. Informația - este o reflectare obiectivă a lumii externe. Informația este obiectivă, în cazul în care nu depinde de metodele sale de stabilire a altcuiva opinii, judecăți.*

*Exemplul * Căldura din stradă» aduce o informație subiectivă , iar mesajul «Afară e 22 ° C» - obiectivă, .Dar, cu precizie, în funcție de mijloacele de erori de măsurare.Informațiile obiective pot fi obținute prin intermediul senzorilor sănătoși si dispozitive de măsurare.*

Reflectate în mintea umană, informațiile pot fi distorsionate (mai mult sau mai puțin), în funcție de punctele de vedere, opiniile, experiențele, cunoștințele unui anumit subiect, și, prin urmare, încetează să mai fie obiectiv.

*2. **Precizia informațiilor**. Informația este viabilă dacă aceasta reflectă adevărata stare a lucrurilor. Informațiile obiective sunt întotdeauna corecte, dar informațiile exacte pot fi obiective și subiective. Informațiile exacte ne ajută să luam decizia corectă. Informațiile false ar putea fi din următoarele motive:*

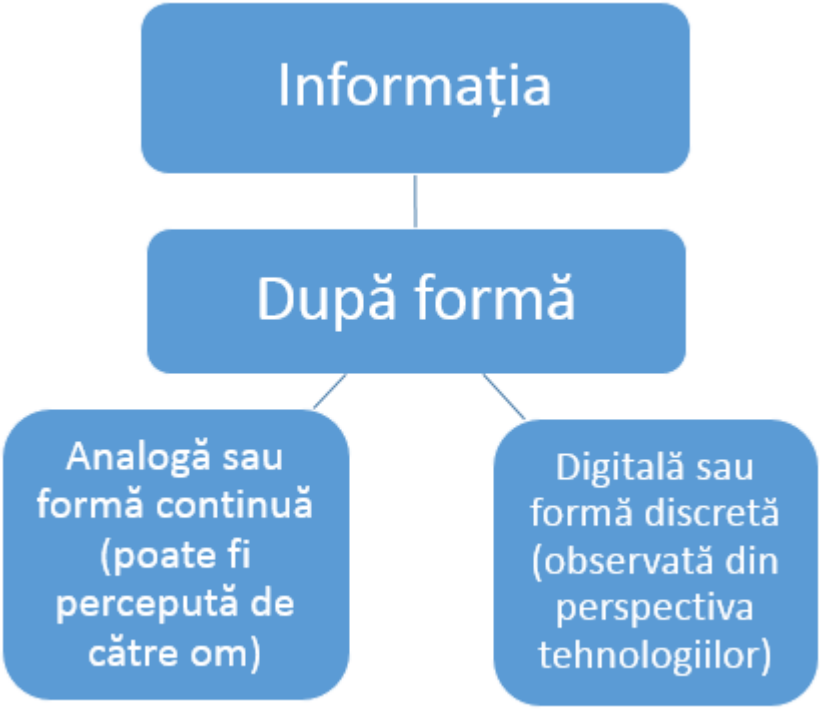
- ✓ *denaturare intenționată (dezinformare) sau o denaturare neintenționată a proprietăților subiective;*
- ✓ *o distorsiune din cauza expunerii la zgomot ("telefon rupt") și mijloace insuficiente de precizie în fixarea acestuia.*

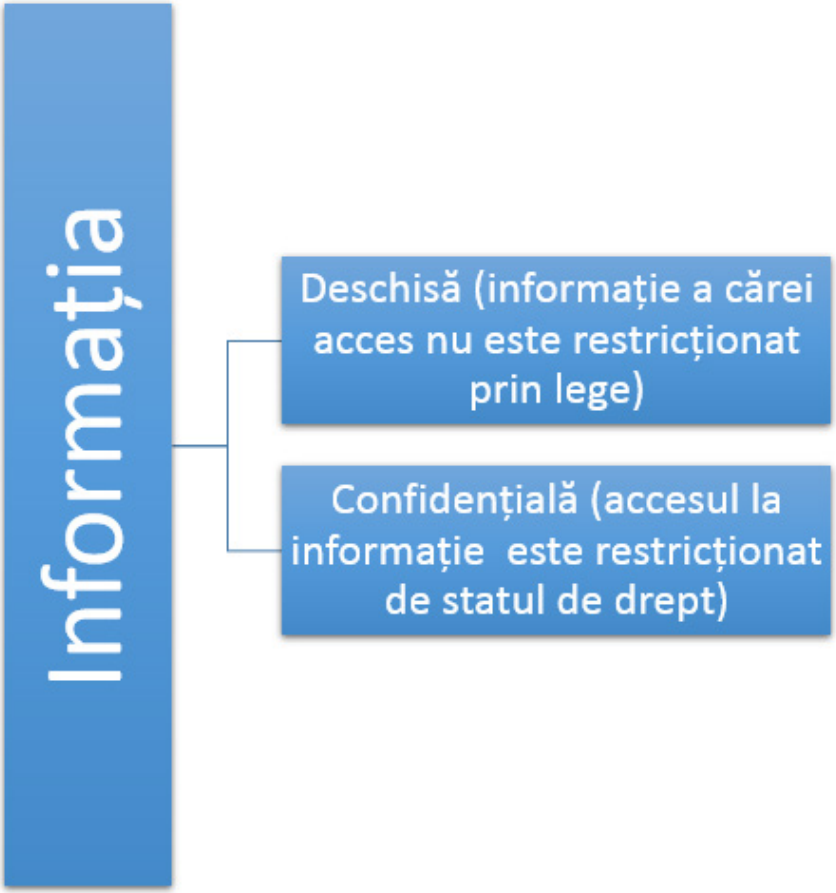
*3. **Integralitatea informației**. Informațiile pot fi numite complete în cazul în care sunt suficiente pentru a înțelege și de a lua decizii. Informațiile incomplete pot duce la concluzii sau decizii greșite .*

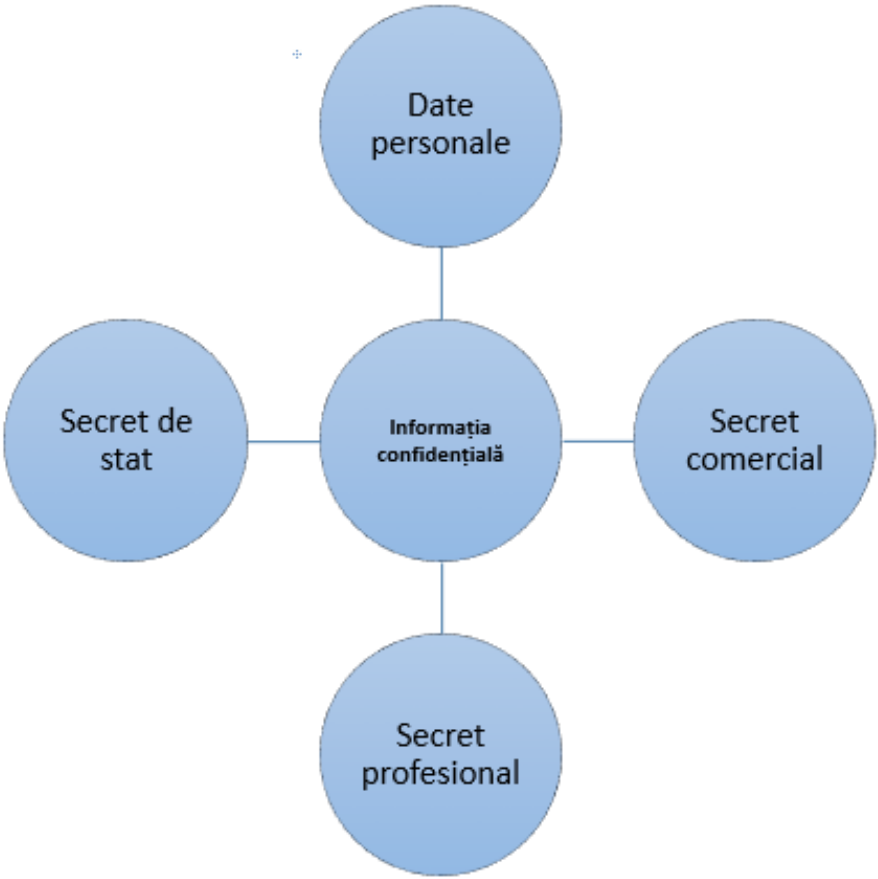
*4. **Precizia informațiilor** este determinată de gradul de proximitatea față de starea actuală a obiectului, procesului , fenomenului , și așa mai departe.*

*5. **Actualitatea informațiilor** - importanța pentru timpul prezent , urgența. Doar din timp obținută informația poate fi de ajutor .*

*6. **Utilitatea (valoarea) informațiilor**. Utilitatea poate fi evaluată în raport cu nevoile specifice ale clienților săi și este apreciată dupa sarcinile care pot fi rezolvate cu ajutorul ei.*


Informația
După formă
Analogă sau formă continuă (poate fi percepută de către om)
Digitală sau formă discretă (observată din perspectiva tehnologiilor)


Informația
Deschisă (informație a cărei acces nu este restricționat prin lege)
Confidențială (accesul la informație este restricționat de statul de drept)


Date personale
Secret de stat
Informația confidențială
Secret comercial
Secret profesional

Informația decshisă

- Reglementată prin Legea nr. 982 din 11.05.2000 "Cu privire la accesul la informație"

Secretul de Stat

- Reglementată prin Legea din 27.11.2008 „Cu privire la secretul de stat”

Date personale

- Reglementate prin Legea nr. 245 din 08.07.2011 "Cu privire la protecția datelor cu caracter personal"

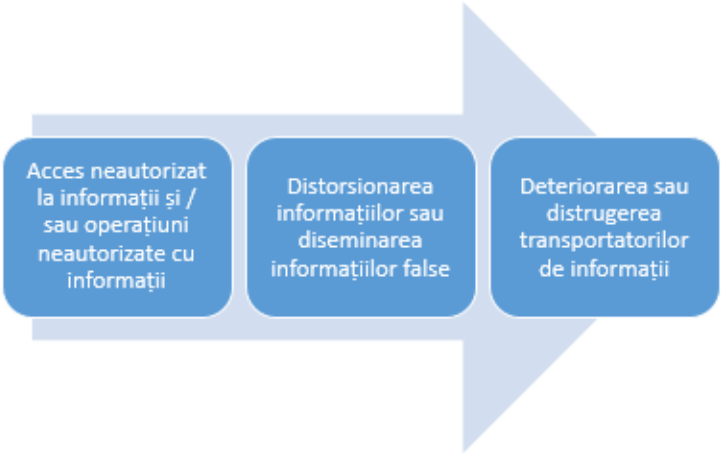
Secret comercial

- Reglementate prin Legea nr. 171 din 06.07.1994 "cu privire la secretul comercial"

Secretul profesional

- Reglementate prin Legea nr. 1260 din 19.07.2002 "despre avocatură”
- Legea nr. 1453 din 08.11.2002 "Cu privire la Notariat"
- Legea nr. 61 din 16.03.2007 "Cu privire la activitatea de audit"
- Lehea Nr. 202 din 06.10.2017 "privind activitatea băncilor"
- Legea nr. 283 din 04.07.2003 "Cu privire la activitatea de detectiv și de securitate privată"
- Legea nr. 264 din 27.10.2005 "Cu privire la activitatea medicală"
- Legea nr. 243 din 26.10.1994 "Cu privire la presă"
- Legea nr. 125 din data de 11.05.2007 "Cu privire la libertate de conștiință, gândire și religie" și alte reglementări.

Amenințările la adresa informației

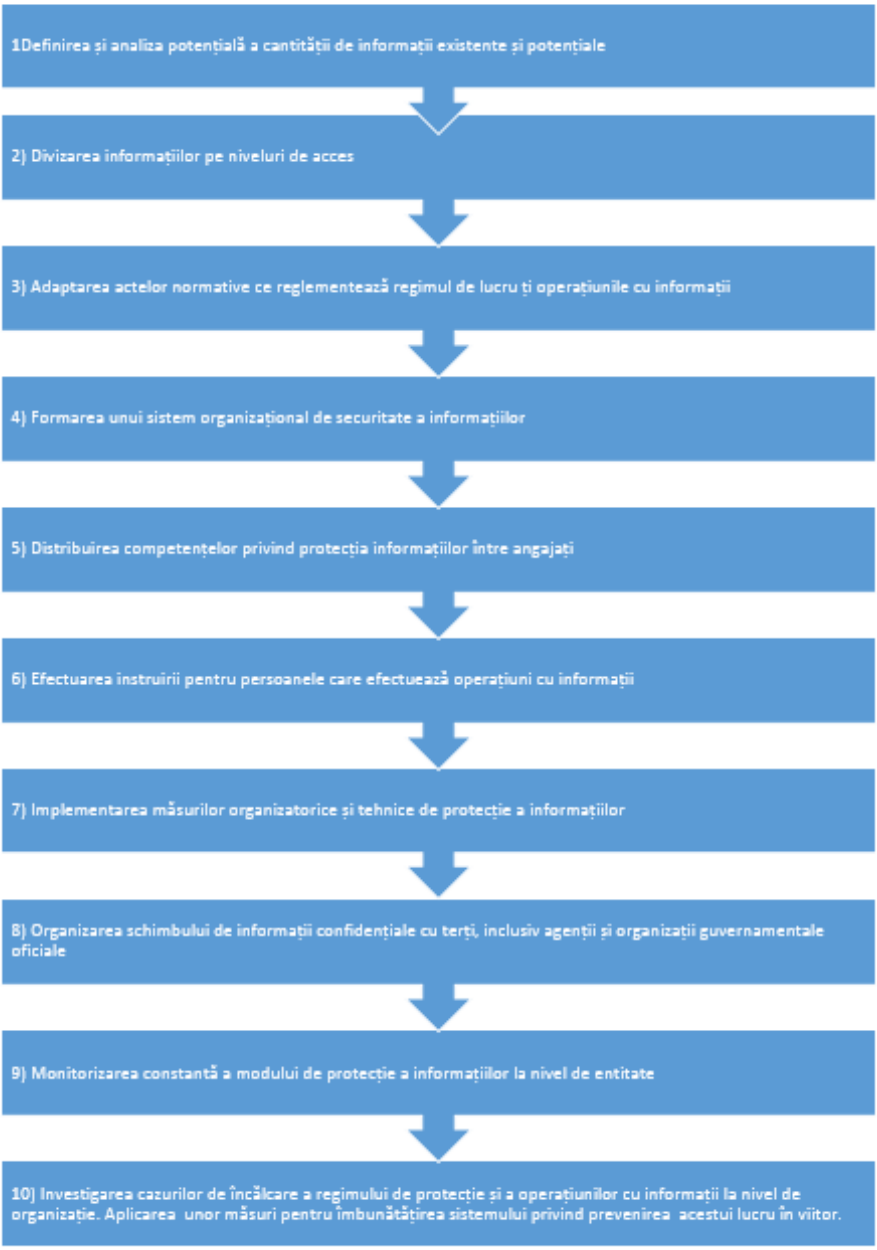


1) Accesul neautorizat la informații și / sau operațiunile neautorizate cu informații sunt una dintre cele mai frecvente amenințări. Acesta este exprimat în obținerea accesului la informații confidențiale ale persoanelor care nu au dreptul de a face acest lucru. Pe lângă familiarizarea neautorizată cu informațiile, aceste persoane pot permite copierea sau transferul informațiilor către alte persoane. Acțiuni similare pot fi, de asemenea efectuate, inclusiv de către persoane cărora li s-a permis accesul la informații, dar nu aveau dreptul de a efectua operațiuni cu informații.
Acces neautorizat este acces la informații efectuat cu încălcarea regimului de lucru

2) Distorsiunea informațiilor este exprimată prin schimbarea deliberată sau accidentală a conținutului sau a sensului informațiilor. Dezinformarea deliberată este acum răspândită și face parte din așa-numitul „război informațional"

3) Deteriorarea sau distrugerea mijloacelor media. Informațiile sunt transmise prin intermediul mass-media, prin urmare, dauna intenționată a mass-media, în cele mai multe cazuri, duce la pierderea parțială, completă sau la denaturarea acesteia.

Procesul de securizare a informației la nivel de entitate



Scurt dicționar terminologic

Informația oficială

- *se considera informatie oficială cea care este deținută în proprietatea și controlul furnizorilor de informații, compilate, selectate, prelucrate, sistematizate și / sau aprobate de către autoritățile, persoane sau sunt puse la dispoziția acestora, în conformitate cu legea celorlalte entități. (Legea nr. 982 din 11.05.2000 despre accesul la informație, articolul 6, paragraful 1)*

Documente cu conținut informativ

- *Acestea se consideră:*
- *1) oricare dintre următorii purtători de informație (sau o parte a acestora):*
- *a) orice hârtie sau alt material pe care înregistrarea este disponibilă;*
- *b) harta, plan, desen, fotografie;*
- *c) orice hârtie sau alt material care conține semne, forme, simboluri sau perforații care sunt relevante pentru persoanele calificate în interpretarea acestora;*
- *d) orice obiect sau material, care poate produce sunete, imagini sau înregistrarea cu un alt obiect sau mecanism;*
- *e) orice alte informații registratorice, care au apărut ca urmare a progresului tehnologic;*
- *2) orice copie sau reproducere a suporturilor de date menționate la punctul 1) din prezenta subsecțiune;*
- *3) o copie a oricărei părți sau de reproducere menționate la punctul*
- *(Legea nr. 982 din 11.05.2000 privind accesul la informație, articolul 6, alineatul 2)*

Date publice

- *datele la care accesul publicului nu este este limitat;(Legea nr. 1069 din 22.06.2000 cu privire la informatica articolul 2)*

Informatica

- *domeniu de activitate,care include prelucrarea și transmiterea datelor cu ajutorul sistemelor informatice automatizate și a comunicațiilor; (Legea nr. 1069 din 22.06.2000 cu privire la informatica articolul 2)*

Informatizarea

- *ansamblu organizat de acţiuni destinate creării, implementării, întreţinerii şi perfecţionării sistemelor automatizate de calcul şi transport de date în procesul de colectare, stocare, prelucrare şi difuzare a informaţiei;*
  (Legea nr. 1069 din 22.06.2000 cu privire la informatica articolul 2)

Informația

- *informații cu privire la persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situații și idei; (Legea nr. 467 din 21.11.2003 privind informatizare și resurselor informaționale de stat articolul 3)*

Suport informațional

- *suport material ale cărui calităţi fizice permit imprimarea, păstrarea şi prelucrarea informaţiei documentate;*
  (Legea nr. 467 din 21.11.2003 privind informatizare și resurselor informaționale de stat articolul 3)

Informaţie cu impact negativ asupra copiilor

- *informaţie accesibilă public care poate fi dăunătoare pentru sănătatea psihică şi fizică a copiilor, pentru dezvoltarea lor fizică, mintală, spirituală şi morală; (Legea nr. 30 din 07.03.2013 cu privire la protecţia copiilor împotriva impactului negativ al informaţiei articolul 1)*

Document electronic

- *informații în format electronic, create, structurate, prelucrate, depozitate și / sau transmise cu ajutorul unui calculator sau alt dispozitiv electronic, semnat de semnătură electronică, în conformitate cu prezenta lege; (Legea nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic articolul 2)*

Semnătura electronică

- *datele în format electronic, care sunt conectate sau asociate cu alte date electronice, în mod logic și utilizate ca metodă de autentificare;(Legea nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic articolul 2)*

Secret de stat

- *informaţii protejate de stat în domeniul apărării naţionale, economiei, ştiinţei şi tehnicii, relaţiilor externe, securităţii statului, asigurării ordinii de drept şi activităţii autorităţilor publice, a căror divulgare neautorizată sau pierdere este de natură să aducă atingere intereselor şi/sau securităţii Republicii Moldova.*
  (Legea nr. 245 din 27.11.2008 cu privire la secretul de stat articolul 1)

Date cu caracter personal

- *date cu caracter personal – orice informaţie referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;*
  categorii speciale de date cu caracter personal – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenenţa socială, datele privind starea de sănătate sau viaţa sexuală, precum şi cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancţiunile contravenţionale;
  (Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal articolul 3)

Prelucrarea datelor cu caracter personal

- orice operaţiune sau serie de operaţiuni 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, ştergerea sau distrugerea;
  (Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal articolul 3)

Operator date cu caracter personal

- *persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituţie ori organizaţie care, în mod individual sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislaţia în vigoare;*
  (Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal articolul 3)

Persoană împuternicită de către operator

- *persoană împuternicită de către operator – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor primite de la operator;*
  (Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal articolul 3)

Obiectele de proprietate intelectuală

- *(1) Se consideră obiect de proprietate intelectuală orice rezultat al activității intelectuale, confirmat și protejat prin drepturile corespunzătoare privind utilizarea acestuia.*
- *(2) Obiectele de proprietate intelectuală se divizează în două categorii: a) obiecte de proprietate industrială (invenții, soiuri de plante, topografii de circuite integrate, mărci, desene și modele industriale, indicații geografice, denumiri de origine și specialități tradiționale garantate); b) obiecte ale dreptului de autor (opere literare, artistice și științifice etc.) și ale drepturilor conexe (interpretări, fonograme, videograme și emisiuni ale organizațiilor de difuziune etc.).*
- *(3) De domeniul proprietății intelectuale țin și alte bunuri ce dispun de un sistem de reglementare separat, cum ar fi: a) secretul comercial (know-how); b) numele comercial.*
- *(4) În cazul obiectelor de proprietate industrială, dreptul asupra acestora apare în urma înregistrării obiectului, a acordării titlului de protecție de către oficiul național de proprietate intelectuală sau în alte condiții prevăzute de legislația națională, precum și în baza tratatelor internaționale la care Republica Moldova este parte. În cazul obiectelor dreptului de autor și ale drepturilor conexe, înregistrarea nu este o condiție obligatorie pentru apariția și exercitarea drepturilor respective, aceste obiecte fiind protejate din momentul creării lor.*
- *(5) În condițiile legii, titularul dreptului asupra obiectului de proprietate intelectuală: a) poate înstrăina dreptul prin cesiune; b) poate permite exploatarea lui de către terți prin licență exclusivă sau neexclusivă; c) poate exercita alte drepturi morale și patrimoniale prevăzute de lege în privința obiectului dreptului exclusiv.*
- *(6) Cu excepțiile prevăzute de lege, nicio persoană nu poate exploata dreptul asupra obiectului de proprietate intelectuală al altuia fără licența corespunzătoare. Licența se prezumă neexclusivă dacă nu s-a prevăzut expres contrariul.*
- *(7) Dreptul asupra obiectului de proprietate intelectuală și dreptul acordat prin licență se consideră bunuri incorporale și pot fi grevate cu drepturi reale limitate în folosul terților. (COD Nr. 1107 06-06-2002 CODUL CIVIL AL REPUBLICII MOLDOVA articolul 476)*

Dobîndirea, utilizarea și divulgarea legală de secrete comerciale

• (1) Dobîndirea unui secret comercial este considerată legală în cazul în care secretul comercial este obținut prin oricare dintre următoarele mijloace:

a) descoperirea sau crearea independentă;

b) analiza, studierea, dezasamblarea sau testarea unui produs sau a unui obiect care a fost făcut public sau care se află în mod legal în posesia celui care a dobîndit informațiile și căruia nu i se aplică nicio obligație validă din punct de vedere legal de a limita dobîndirea secretului comercial;

c) exercitarea dreptului salariaților sau al reprezentanților salariaților la informare și la consultare în conformitate cu legislația;

d) orice altă practică care, în circumstanțele date, este conformă cu practicile comerciale loiale.

(2) Dobîndirea, utilizarea sau divulgarea unui secret comercial este considerată legală în măsura în care aceasta dobîndire, utilizare sau divulgare este impusă sau permisă în temeiul legislației.

(COD Nr. 1107 06-06-2002 CODUL CIVIL AL REPUBLICII MOLDOVA articolul 2045)

Dobîndirea, utilizarea și divulgarea ilegală de secrete comerciale

• (1) Dobîndirea unui secret comercial fără consimțămîntul deținătorului secretului comercial este considerată ilegală ori de cîte ori este efectuată prin:

a) accesul neautorizat, însușirea sau copierea oricăror documente, obiecte, materiale, substanțe sau fișiere electronice care se află în mod legal sub controlul deținătorului secretului comercial și care conțin secretul comercial sau din care poate fi dedus secretul comercial;

b) orice alt comportament care, în circumstanțele date, este considerat contrar practicilor comerciale loiale.

(2) Utilizarea sau divulgarea unui secret comercial este considerată ilegală ori de cîte ori este săvîrșită, fără consimțămîntul deținătorului secretului comercial, de către o persoană care îndeplinește oricare dintre următoarele condiții:

a) a dobîndit secretul comercial în mod ilegal;

b) încalcă un contract de confidențialitate sau orice altă obligație de a nu divulga secretul comercial;

c) încalcă o obligație contractuală sau de altă natură care limitează utilizarea secretului comercial.

(3) Dobîndirea, utilizarea sau divulgarea unui secret comercial este, de asemenea, considerată ilegală atunci cînd o persoană, în momentul dobîndirii, utilizării sau divulgării, avea cunoștință sau ar fi trebuit să aibă cunoștință, în circumstanțele date, de faptul că secretul comercial a fost obținut, direct sau indirect, de la o altă persoană care a utilizat sau a divulgat secretul comercial în mod ilegal în sensul lin. (2).

(4) Producerea, oferirea sau introducerea pe piață a mărfurilor care încalcă secretul comercial sau importul, exportul sau depozitarea unor astfel de mărfuri în aceste scopuri este, de asemenea, considerată utilizare ilegală a unui secret comercial atunci cînd persoana care desfășoară astfel de activități avea cunoștință sau ar fi trebuit să aibă cunoștință, în circumstanțele date, de faptul că secretul comercial a fost utilizat în mod ilegal în sensul alin. (2).

(5) În sensul prezentei legi, se consideră mărfuri care încalcă secretul comercial mărfurile a căror concepere, caracteristici, funcționare, proces de producție sau comercializare beneficiază în mod semnificativ de secrete comerciale obținute, utilizate sau divulgate în mod ilegal.

(LEGE Nr. 3307 06-06-2002 CODUL CIVIL AL REPUBLICII MOLDOVA articolul 2046)

Secretul avocaturii

- *(1) Avocatul nu este în drept să divulge informaţiile confidenţiale ce i-au fost comunicate în timpul acordării asistenţei juridice, precum şi să transmită, fără acordul clientului, unor terţi documentele legate de exercitarea delegaţiei.*
- *(2) Obligaţia de a păstra secretul profesional nu este limitată în timp.*
  (Legea Nr. 1260 din 19-07-2002 cu privire la avocatură articolul 55)

Secretul profesional al notarului

- *Notarul este obligat să păstreze secretul profesional cu privire la actele îndeplinite şi faptele ce i-au devenit cunoscute în cadrul activităţii sale, indiferent de modul de obţinere ori sursa informaţiei, inclusiv după încetarea activităţii sale.*
  (Legea r. 69 din 14-04-2016 cu privire la organizarea activităţii notarilor articolul7.)

Confidenţialitatea şi secretul profesional al auditorului

- *1) Auditorul și entitatea de audit respectă confidențialitatea și secretul profesional privind informațiile referitoare la activitatea entității auditate, obținute în timpul exercitării auditului. Obligația de a respecta confidențialitatea și secretul profesional rămîne în vigoare și după încetarea contractului de audit.*
  (2) Auditorul și entitatea de audit asigură respectarea confidențialității și a secretului profesional și din partea personalului care își desfășoară activitatea sub controlul său, precum și din partea persoanelor care oferă consultanță și asistență.
  (Legea nr 271 din 15-12-2017 privind auditul situațiilor financiare articolul 22)

Secretul bancar

- *(1) Banca este obligată să păstreze confidenţialitatea asupra tuturor faptelor, datelor şi informaţiilor referitoare la activitatea sa, precum şi asupra oricăror fapte, date sau informaţii, aflate la dispoziţia sa, referitoare la persoana, bunurile, activitatea, afacerea, relaţiile personale sau de afaceri ale clienţilor băncii ori informaţiile referitoare la conturile clienţilor (solduri, rulaje, operaţiuni derulate), tranzacţiile încheiate de clienţi, precum şi a altor informaţii despre clienţi care i-au devenit cunoscute.*
  (Legea nr. 202 din 06.10.2017 privind activitatea băncilor articolul 96)

Secretul profesional al Băncii Naţionale a Moldovei

- *((1) Membrii organelor de conducere şi salariaţii Băncii Naţionale a Moldovei, precum şi salariaţii societăţilor de audit sau experţii numiţi de Banca Naţională a Moldovei pentru efectuarea de verificări la sediul băncilor, potrivit prevederilor art.106 alin.(5), sînt obligaţi să păstreze secretul profesional asupra oricărei informaţii confidenţiale de care iau cunoştinţă în cursul exercitării atribuţiilor lor în aplicarea prezentei legi. Membrii organelor de conducere şi salariaţii Băncii Naţionale a Moldovei sînt obligaţi să păstreze secretul profesional şi după încetarea activităţii în cadrul băncii.*
- *(2) Persoanele prevăzute la alin.(1) nu pot divulga informaţii confidenţiale niciunei persoane sau autorităţi, cu excepţia furnizării acestor informaţii în formă sumară sau agregată, astfel încît banca să nu poată fi identificată.*
- *În sensul prezentului capitol, informaţiile confidenţiale înseamnă orice informaţii ce reprezintă secret bancar, comercial, fiscal şi alt secret ocrotit de lege, precum şi informaţiile create de către Banca Naţională a Moldovei în scopul ori în legătură cu exercitarea atribuţiilor ei, a căror divulgare ar putea dăuna interesului sau prestigiului persoanei la care se referă.(Legea nr. 202 din 06.10.2017 privind activitatea băncilor articolul 126)*

Secretul profesional al persoanelor care practică activitate particulară de detectiv şi de pază

- *Persoana care practică activitate particulară de detectiv şi de pază este obligată:să păstreze confidenţialitatea informaţiei pe care o cunoaşte în procesul activităţii, să nu o utilizeze în scopuri personale şi să nu o transmită terţilor;*
  (Legea nr. 283 din 04-07-2003 privind activitatea particulară de detectiv şi de pază articolul 8)

Secretul profesional al părților medicale

- *(1) Medicul este obligat să păstreze secretul profesional.*
- *(2) Informațiile despre solicitarea asistenței medicale, despre starea sănătății, diagnostic și alte date obținute de medic în examinarea și tratamentul pacientului constituie informații personale și secretul profesional al medicului și nu pot fi divulgate.(Legea nr. r. 264 din 27-10-2005 cu privire la exercitarea profesiunii de medic articolul 13)*

Secretul profesional al jurnalistului

- *În scopul de a desfășura activități profesionale, jurnalistul are dreptul de a pretinde la calitatea de autor al secretului. (Legea nr. 243 din 26.10.1994 privind presa articolul 20).*
- *(1) Publicațiile periodice și agențiile de presă publică, potrivit aprecierilor proprii, orice fel de materiale și informații, ținînd cont de faptul că exercițiul acestor libertăți ce comportă datorii și responsabilități este supus unor formalități, condiții, restrîngeri și unor sancțiuni prevăzute de lege, care constituie măsuri necesare, într-o societate democratică, pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii și prevenirea crimei, ocrotirea sănătății, protecția moralei, protecția reputației sau apărarea drepturilor altora, pentru a împiedica divulgarea unor informații confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judiciare.*
  (2) Publicațiile periodice și agențiile de presă sînt obligate să utilizeze un limbaj accesibil și să prezinte informația furnizată în așa mod încît aceasta să nu lezeze onoarea și demnitatea persoanelor cu dizabilități.
  (3) Este inadmisibilă și se contracarează în conformitate cu legislația în vigoare publicarea oricăror materiale și informații care prezintă imaginea persoanelor cu dizabilități în manieră de umilință a demnității și/sau conține un îndemn deschis sau ascuns la discriminare, ură și la alte acțiuni ce ar încălca drepturile acestor persoane.(Legea nr. 243 din 26.10.1994 privind presa articolul 4).

Secretul mărturisirii

- *Secretul spovedaniei este protejat prin lege. Slujitorii de cult religios sunt obligați să păstreze secretul spovedaniei și nu poate fi obligat să-l dezvăluie.(Legea nr. 125 din 11.05.2007 cu privire la libertatea de conștiință, gândire și religie Articolul 11)*

Declarația universală a drepturilor omului

Adoptat prin Rezoluția Adunării Generale 217 A (III) a Adunării Generale a ONU la 10 decembrie anul 1948

- ***Articolul 12***
  Nimeni nu va fi supus la imixtiuni arbitrare în viaţa sa personală, în familia sa, în domiciliul lui sau în corespondenţa sa, nici la atingeri aduse onoarei şi reputaţiei sale. Orice persoană are dreptul la protecţia legii împotriva unor asemenea imixtiuni sau atingeri.

- ***Articolul 19***
  Orice om are dreptul la libertatea opiniilor şi exprimării; acest drept include libertatea de a avea opinii fără fără imixtiune din afară,precum şi libertatea de a căuta, de a primi şi de a răspîndi informaţii şi idei prin orice mijloace si independent de frontierele de stat.

Constituția Republicii Moldova din 29.07.1994

- ***Articolul 30***
- ***Secretul corespondenței***
- *(1) Statul asigură secretul scrisorilor, al telegramelor, al altor trimiteri poştale, al convorbirilor telefonice şi al celorlalte mijloace legale de comunicare.*
- *(2) De la prevederile alineatului (1) se poate deroga prin lege în cazurile cînd această derogare este necesară în interesele securităţii naţionale, bunăstării economice a ţării, ordinii publice şi în scopul prevenirii infracţiunilor.*

- ***Articolul 34***
- ***Dreptul la informație***
- *(1) Dreptul persoanei de a avea acces la orice informație de interes public nu poate fi îngrădit.*
- *(2) Autoritățile publice, potrivit competențelor ce le revin, sînt obligate să asigure informarea corectă a cetățenilor asupra treburilor publice și asupra problemelor de interes personal.*
- *(3) Dreptul la informație nu trebuie să prejudicieze măsurile de protecție a cetățenilor sau siguranța națională.*
- *(4) Mijloacele de informare publică, de stat sau private, sînt obligate să asigure informarea corectă a opiniei publice.*
- *(5) Mijloacele de informare publică nu sînt supuse cenzurii.*

- ***Articolul 54***
- ***Restrîngerea exercițiului unor drepturi sau al unor libertăți***
- *(1) În Republica Moldova nu pot fi adoptate legi care ar suprima sau ar diminua drepturile și libertățile fundamentale ale omului și cetățeanului.*
- *(2) Exercițiul drepturilor și libertăților nu poate fi supus altor restrîngeri decît celor prevăzute de lege, care corespund normelor unanim recunoscute ale dreptului internațional și sînt necesare în interesele securității naționale, integrității teritoriale, bunăstării economice a țării, ordinii publice, în scopul prevenirii tulburărilor în masă și infracțiunilor, protejării drepturilor, libertăților și demnității altor persoane, împiedicării divulgării informațiilor confidențiale sau garantării autorității și imparțialității justiției.*
- *(3) Prevederile alineatului (2) nu admit restrîngerea drepturilor proclamate în articolele 2024.*
- *(4) Restrîngerea trebuie să fie proporțională cu situația care a determinato și nu poate atinge existența dreptului sau a libertății.*

PARLAMENTUL

LEGE Nr. 982 din 11-05-2000

privind accesul la informaţie

Publicat : 28-07-2000 în Monitorul Oficial Nr. 88-90 art. 664

MODIFICAT LP143 din 19.07.18, MO309-320/17.08.18

Articolul 1. Obiectul de reglementare al prezentei legi

(1) Prezenta lege reglementează:

raporturile dintre furnizorul de informaţii şi persoana fizică si/sau juridică în procesul de asigurare şi realizare a dreptului constituţional de acces la informaţie;

b) principiile, condiţiile, căile şi modul de realizare a accesului la informaţiile oficiale, aflate în posesia furnizorilor de informaţii;

e) obligaţiile furnizorilor de informaţii în procesul asigurării accesului la informaţiile oficiale;

f) modalitatea apărării dreptului de acces la informaţie.

(2) Nu constituie obiect al prezentei legi raporturile care au legătură tangenţială cu raporturile enumerate în alineatul (1) al prezentului articol şi se referă la:

a) colectarea, prelucrarea, depozitarea şi garantarea integrităţii informaţiilor;

b) prezentarea obligatorie a informaţiilor prevăzute de lege de către persoane private autorităţilor publice, instituţiilor publice;

c) accesul autorităţilor publice, instituţiilor publice, persoanelor fizice şi/sau juridice, abilitate cu gestionarea unor servicii publice, la informaţiile aflate în posesia altor asemenea autorităţi publice, instituţii publice, persoane fizice şi/sau juridice;

d) furnizarea informaţiilor referitoare la propria activitate de către persoane fizice şi juridice private, partide şi formaţiuni social-politice, fundaţii, asociaţii obşteşti.

Articolul 2. Obiectivele prezentei legi

Prezenta lege are drept scop:

a) crearea cadrului normativ general al accesului la informaţiile oficiale;

b) eficientizarea procesului de informare a populaţiei şi a controlului efec-

tuat de către cetăţeni asupra activităţii autorităţilor publice şi a instituţiilor publice;

c) stimularea formării opiniilor şi participării active a populaţiei la procesul de luare a deciziilor în spirit democratic.

Articolul 3. Legislaţia privind accesul la informaţie

(1) Legislaţia privind accesul la informaţie are la bază Constituţia Republicii Moldova, tratatele şi acordurile internaţionale la care Republica Moldova este parte, prezenta lege şi include prevederile altor acte normative care reglementează raporturile ce ţin de accesul la informaţie.

(2) Dacă tratatul sau acordul internaţional la care Republica Moldova este parte stabileşte alte norme decît cele cuprinse în legislaţia naţională, se aplică normele tratatului sau acordului internaţional.

Articolul 4. Principiile politicii statului în domeniul accesului la informaţiile oficiale

(1) Oricine, în condiţiile prezentei legi, are dreptul de a căuta, de a primi şi de a face cunoscute informaţiile oficiale.

(2) Exercitarea drepturilor prevăzute în alineatul (1) al prezentului articol poate fi supusă unor restricţii pentru motive specifice, ce corespund principiilor dreptului internaţional, inclusiv pentru apărarea securităţii naţionale sau vieţii private a persoanei.

(3) Exercitarea drepturilor prevăzute la alineatul (1) al prezentului articol nu va implica în nici un caz discriminarea bazată pe rasă, naţionalitate, origine etnică, limbă, religie, sex, opinie, apartenenţă politică, avere sau pe origine socială.

Articolul 5. Subiecţii prezentei legi

(1) Subiecţi ai prezentei legi sînt furnizorul de informaţii şi solicitantul informaţiei.

(2) Furnizori de informaţii, adică posesori ai informaţiilor oficiale, obligaţi să le furnizeze solicitanţilor în condiţiile prezentei legi, sînt:

a) autorităţile publice centrale şi locale - autorităţile administraţiei de stat, prevăzute în Constituţia Republicii Moldova şi anume: Parlamentul, Preşedintele Republicii Moldova, Guvernul, administraţia publică, autoritatea judecătorească;

b) instituţiile publice centrale şi locale - organizaţiile fondate de către stat în persoana autorităţilor publice şi finanţate de la bugetul de stat, care au ca scop efectuarea atribuţiilor de administrare, social-culturale şi altor atribuţii cu caracter necomercial;

c) persoanele fizice şi juridice care, în baza legii sau a contractului cu autoritatea publică ori instituţia publică, sînt abilitate cu gestionarea unor servicii publice şi culeg, selectează, posedă, păstrează, dispun de informaţii oficiale.

(3) Pot solicita informaţii oficiale, în condiţiile prezentei legi:

a) orice cetăţean al Republicii Moldova;

b) cetăţenii altor state, care au domiciliul sau reşedinţa pe teritoriul Republicii Moldova;

c) apatrizii stabiliţi cu domiciliul sau cu reşedinţa pe teritoriul Republicii Moldova.

Articolul 6. Informaţiile oficiale

(1) În sensul prezentei legi, informaţii oficiale sînt considerate toate informaţiile aflate în posesia şi la dispoziţia furnizorilor de informaţii, care au fost elaborate, selectate, prelucrate, sistematizate şi/sau adoptate de organe ori persoane oficiale sau puse la dispoziţia lor în condiţiile legii de către alţi subiecţi de drept.

(2) În sensul prezentei legi, drept documente purtătoare de informaţii sînt considerate:

1) oricare din următoarele (sau o parte din acestea):

a) orice hîrtie sau alt material pe care există un înscris;

b) o hartă, un plan, un desen, o fotografie;

c) orice hîrtie sau alt material pe care sînt marcaje, figuri, simboluri sau perforări care au un sens pentru persoanele calificate să le interpreteze;

d) orice obiect sau material din care pot fi reproduse sunete, imagini sau înscrisuri cu sau fără ajutorul unui alt articol sau mecanism;

e) orice alt înregistrator de informaţie apărut ca rezultat al progresului tehnic;

2) orice copie sau reproducere a purtătorilor de informaţii menţionaţi la punctul 1) al prezentului alineat;

3) orice parte a unei copii sau reproduceri menţionate la punctul 2) al prezentului alineat.

(3) Informaţiile oficiale nedocumentate, care se află în posesia furnizorilor (persoanelor responsabile ale acestora), vor fi puse la dispoziţia solicitanţilor în ordine generală.

Articolul 7. Informaţiile oficiale cu accesibilitate limitată

(1) Exercitarea dreptului de acces la informaţie poate fi supusă doar restricţiilor reglementate prin lege organică şi care corespund necesităţilor:

a) respectării drepturilor şi reputaţiei altei persoane;

b) protecţiei securităţii naţionale, ordinii publice, ocrotirii sănătăţii sau protecţiei moralei societăţii.

(2) În conformitate cu alineatul (1) al prezentului articol, accesul la informaţiile oficiale nu poate fi îngrădit, cu excepţia:

a) informaţiilor atribuite la secret de stat, reglementate prin lege organică, a căror divulgare neautorizată sau pierdere poate aduce atingere intereselor şi/sau securităţii Republicii Moldova;

b) informaţiilor confidenţiale din domeniul afacerilor, prezentate instituţiilor publice cu titlu de confidenţialitate, reglementate de legislaţia privind secretul comercial, şi care ţin de producţie, tehnologie, administrare, finanţe, de altă activitate a vieţii economice, a căror divulgare (transmitere, scurgere) poate atinge interesele întreprinzătorilor;

c) informaţiilor cu caracter personal, a căror divulgare este considerată drept o imixtiune în viaţa privată a persoanei, protejată de legislaţia privind protecţia datelor cu caracter personal;

d) informaţiilor ce ţin de activitatea operativă şi de urmărire penală a organelor de resort, dar numai în cazurile în care divulgarea acestor informaţii ar putea prejudicia urmărirea penală, interveni în desfăşurarea unui proces de judecată, lipsi persoana de dreptul la o judecare corectă şi imparţială a cazului său, ori ar pune în pericol viaţa sau securitatea fizică a oricărei persoane - aspecte reglementate de legislaţie;

e) informaţiilor ce reflectă rezultatele finale sau intermediare ale unor investigaţii ştiinţifice şi tehnice şi a căror divulgare privează autorii investigaţiilor de prioritatea de publicare sau influenţează negativ exercitarea altor drepturi protejate prin lege.

(3) Dacă accesul la informaţiile, documentele solicitate este parţial limitat, furnizorii de informaţii sînt obligaţi să prezinte solicitanţilor părţile documentului, accesul la care nu conţine restricţii conform legislaţiei, indicîndu-se în locurile porţiunilor omise una din următoarele sintagme: „secret de stat”, „secret comercial”, „informaţie confidenţială despre persoană”. Refuzul accesului la informaţie, la părţile respective ale documentului se întocmeşte cu respectarea prevederilor articolului 19 din prezenta lege.

(4) Nu se vor impune restricţii ale libertăţii de informare decît dacă furnizorul de informaţii poate demonstra că restricţia este reglementată prin lege organică şi necesară într-o societate democratică pentru apărarea drepturilor şi intereselor legitime ale persoanei sau protecţiei securităţii naţionale şi că prejudiciul adus acestor drepturi şi interese ar fi mai mare decît interesul public în cunoaşterea informaţiei.

(5) Nimeni nu poate fi pedepsit pentru că a făcut publice anumite informaţii cu accesibilitate limitată, dacă dezvăluirea informaţiilor nu atinge şi nu poate să atingă un interes legitim legat de securitatea naţională sau dacă interesul public de a cunoaşte informaţia depăşeşte atingerea pe care ar putea să o aducă dezvăluirea informaţiei.

Articolul 8. Accesul la informaţia cu caracter personal

(1) Informaţia cu caracter personal face parte din categoria informaţiei oficiale cu accesibilitate limitată şi constă din date referitoare la o persoană fizică identificată sau identificabilă, a căror dezvăluire ar constitui o violare a vieţii private, intime şi familiale.

(2) Accesul la informaţia cu caracter personal se realizează în conformitate cu prevederile legislaţiei privind protecţia datelor cu caracter personal.

Articolul 9. Accesul la informaţia păstrată în Fondul Arhivistic al Republicii Moldova

(1) Modalitatea accesului la informaţia păstrată în Fondul Arhivistic al Republicii Moldova este reglementată de Legea privind Fondul Arhivistic al Republicii Moldova şi de prezenta lege.

(2) În caz de neconcordanţe între prevederile prezentei legi şi cele ale Legii privind Fondul Arhivistic al Republicii Moldova, se vor aplica dispoziţiile prezentei legi.

Articolul 10. Drepturile solicitanţilor

(1) Persoana are dreptul de a solicita furnizorilor de informaţii, personal sau prin reprezentanţii săi, orice informaţii aflate în posesia acestora, cu excepţiile stabilite de legislaţie.

(2) Dreptul persoanei de a avea acces la informaţii, inclusiv la informaţiile cu caracter personal, nu poate fi îngrădit decît în condiţiile legii.

(3) Orice persoană care solicită acces la informaţii în conformitate cu prezenta lege este absolvită de obligaţia de a-şi justifica interesul pentru informaţiile solicitate.

Articolul 11. Obligaţiile furnizorului de informaţii

(1) Furnizorul de informaţii, în conformitate cu competenţele care îi revin, este obligat:

1) să asigure informarea activă, corectă şi la timp a cetăţenilor asupra chestiunilor de interes public şi asupra problemelor de interes personal;

2) să garanteze liberul acces la informaţie;

3) să respecte limitările accesului la informaţie, prevăzute de legislaţie, în scopul protejării informaţiei confidenţiale, vieţii private a persoanei şi securită-

ţii naţionale;

4) să respecte termenele de furnizare a informaţiei, prevăzute de lege;

5) să dea publicităţii propriile acte adoptate în conformitate cu legea;

6) să păstreze, în termenele stabilite de lege, propriile acte, actele instituţiilor, ale căror succesoare sînt, actele ce stabilesc statutul lor juridic;

7) să asigure protejarea informaţiilor ce se află la dispoziţia sa de accesul, distrugerea sau modificarea nesancţionate;

8) să menţină informaţiile, documentele aflate la dispoziţia sa, în formă actualizată;

9) să difuzeze de urgenţă pentru publicul larg informaţia care i-a devenit cunoscută în cadrul propriei activităţi, dacă această informaţie:

a) poate preîntîmpina sau diminua pericolul pentru viaţa şi sănătatea oamenilor;

b) poate preîntîmpina sau diminua pericolul producerii unor prejudicii de orice natură;

c) poate opri răspîndirea informaţiei neveridice sau diminua consecinţele negative ale răspîndirii acesteia;

d) comportă o deosebită importanţă socială.

10) să asigure furnizarea datelor din registrele de stat prin intermediul platformei de interoperabilitate.

[Art.11 al.(1), pct.10) introdus prin LP143 din 19.07.18, MO309-320/17.08.18 art.482; în vigoare 10.11.18]

(2) în scopul garantării liberului acces la informaţiile oficiale, furnizorul de informaţii:

a) va asigura un spaţiu amenajat pentru documentare, accesibil solicitanţilor;

b) va numi şi va instrui funcţionarii responsabili pentru efectuarea procedurilor de furnizare a informaţiilor oficiale;

c) va elabora, în conformitate cu prezenta lege, regulamente cu privire la drepturile şi obligaţiile funcţionarilor în procesul de furnizare a documentelor, informaţiilor oficiale;

d) va acorda asistenţa şi sprijinul necesar solicitanţilor pentru căutarea şi identificarea informaţiilor;

e) va asigura accesul efectiv la registrele furnizorilor de informaţii, care vor fi completate în conformitate cu legislaţia cu privire la registre;

e) va asigura accesul efectiv, prin intermediul platformei de interoperabilitate, la registrele furnizorilor de informaţii, care vor fi completate în conformitate cu legislaţia cu privire la registre;

[Art.11 al.(2), lit.e) modificată prin LP143 din 19.07.18, MO309-320/17.08.18 art.482; în vigoare 10.11.18]

f) va desfăşura întrunirile şi şedinţele sale în mod public, în conformitate cu legislaţia.

(3) în scopul facilitării liberului acces la informaţie, furnizorul de informaţii va publica sau va face în alt mod general şi direct accesibile populaţiei informaţiile ce conţin:

a) descrierea structurii instituţiei şi adresa acesteia;

b) descrierea funcţiilor, direcţiilor şi formelor de activitate ale instituţiei;

c) descrierea subdiviziunilor cu competenţele lor, programului de lucru al acestora, cu indicarea zilelor şi orelor de audienţă a funcţionarilor responsabili de furnizarea informaţiilor, documentelor oficiale;

d) deciziile finale asupra principalelor probleme examinate.

(4) În conformitate cu prezenta lege, informaţiile arătate la alineatul (3) al prezentului articol vor fi făcute publice în afara procedurii de examinare a cererilor privind accesul la informaţie.

(5) În scopul asigurării transparenţei activităţii instituţiilor, eficientizării accesului la informaţie, creării condiţiilor pentru căutarea, identificarea operativă a documentelor şi informaţiilor, autorităţile publice, instituţiile publice vor edita, cel puţin o dată pe an, îndrumare ce vor conţine liste ale dispoziţiilor, hotărîrilor, altor documente oficiale, emise de instituţia respectivă, şi domeniile în care poate furniza informaţii, vor pune la dispoziţia reprezentanţilor mijloacelor de informare în masă date oficiale despre propria activitate, inclusiv despre domeniile în care poate furniza informaţii.

(6) Furnizorul de informaţii va proceda şi la alte forme de informare activă a cetăţenilor şi a mijloacelor de informare în masă.

Articolul 12. Solicitarea accesului la informaţiile oficiale

(1) Informaţiile oficiale vor fi puse la dispoziţia solicitanţilor în baza unei cereri scrise sau verbale.

(2) Cererea scrisă va conţine:

a) detalii suficiente şi concludente pentru identificarea informaţiei solicitate (a unei părţi sau unor părţi ale acesteia);

b) modalitatea acceptabilă de primire a informaţiei solicitate;

c) date de identificare ale solicitantului.

(4) Cererea poate fi înaintată verbal în cazurile în care este posibil răspunsul pozitiv, cu satisfacerea imediată a cererii de furnizare a informaţiei. În cazul în care furnizorul intenţionează să refuze accesul la informaţia solicitată, el va informa solicitantul despre aceasta şi despre posibilitatea depunerii unei cereri scrise.

(5) Elaborarea şi furnizarea unor informaţii analitice, de sinteză sau inedite pot fi efectuate în baza unui contract între solicitant şi furnizorul de informaţii, contra unei plăţi negociabile, dacă furnizorul va fi disponibil şi în drept să realizeze o asemenea ofertă.

Articolul 13. Modalităţile accesului la informaţiile oficiale

(1) Modalităţile accesului la informaţiile oficiale sînt:

a) audierea informaţiei pasibile de o expunere verbală;

b) examinarea documentului (unor părţi ale acestuia) la sediul instituţiei;

c) eliberarea copiei de pe documentul, informaţia solicitate (de pe unele părţi ale acestora);

d) eliberarea copiei traducerii documentului, informaţiei (unor părţi ale acestora) într-o altă limbă decît cea a originalului, pentru o plată suplimentară;

e) expedierea prin poştă (inclusiv poşta electronică) a copiei de pe document, informaţie (de pe unele părţi ale acestora), copiei de pe traducerea documentului, informaţiei într-o altă limbă, la cererea solicitantului, pentru o plată respectivă.

(2) Extrasele din registre, documente, informaţii (unele părţi ale acestora), în conformitate cu cererea solicitantului, pot fi puse la dispoziţia persoanei date, într-o formă rezonabilă şi acceptabilă pentru aceasta, spre a fi:

a) examinate la sediul instituţiei;

b) dactilografiate, fotocopiate sau copiate într-o altă modalitate ce ar asigura integritatea originalului;

c) înscrise pe un purtător electronic, imprimate pe casete video, audio, alt purtător rezultat din progresul tehnic.

Articolul 14. Limba în care se vor prezenta informaţiile solicitate

(1) Informaţiile, documentele, solicitate în conformitate cu prezenta lege, vor fi puse la dispoziţia solicitanţilor în limba de stat sau în limba în care au fost elaborate.

(2) În cazul în care informaţiile, documentele au fost elaborate într-o altă limbă decît cea de stat, furnizorul de informaţii va fi obligat să prezinte, la ce-

rerea solicitantului, o copie a traducerii autentice a informaţiei, documentului în limba de stat.

Articolul 15. Examinarea cererilor privind accesul la informaţie

(1) Cererile scrise cu privire la accesul la informaţie vor fi înregistrate în conformitate cu legislaţia cu privire la registre şi petiţionare.

(2) Cererile respective vor fi examinate şi satisfăcute de funcţionarii publici responsabili de furnizarea informaţiilor.

(3) Deciziile, luate în conformitate cu prezenta lege, vor fi comunicate solicitantului într-un mod ce ar garanta recepţionarea şi conştientizarea acestora.

(4) În cadrul satisfacerii cererii privind accesul la informaţie, furnizorii vor lua toate măsurile necesare pentru nedivulgarea informaţiilor cu acces limitat, pentru protecţia integrităţii informaţiilor şi excluderea accesului nesancţionat la ele.

Articolul 16. Termenele de satisfacere a cererilor de acces la informaţie

(1) Informaţiile, documentele solicitate vor fi puse la dispoziţia solicitantului din momentul în care vor fi disponibile pentru a fi furnizate, dar nu mai tîrziu de 15 zile lucrătoare de la data înregistrării cererii de acces la informaţie.

(2) Termenul de furnizare a informaţiei, documentului poate fi prelungit cu 5 zile lucrătoare de către conducătorul instituţiei publice dacă:

a) cererea se referă la un volum foarte mare de informaţii care necesită selectarea lor;

b) sînt necesare consultaţii suplimentare pentru a satisface cererea.

(3) Autorul cererii va fi informat despre orice prelungire a termenului de furnizare a informaţiei şi despre motivele acesteia cu 5 zile înainte de expirarea termenului iniţial.

Articolul 17. Readresarea cererilor

Cererea de furnizare a informaţiei poate fi readresată altui furnizor, cu informarea obligatorie a solicitantului în decurs de 3 zile lucrătoare de la momentul primirii cererii şi cu acordul solicitantului, în următoarele cazuri:

a) informaţia solicitată nu se află în posesia furnizorului sesizat;

b) informaţia solicitată deţinută de alt furnizor ar satisface mai deplin interesul faţă de informaţie al solicitantului.

Articolul 18. Eliberarea informaţiilor oficiale

Informaţiile oficiale, documentele, părţile acestora, extrasele din registre, copiile traducerilor, eliberate conform prezentei legi, vor fi semnate de persoana responsabilă.

Articolul 19. Refuzul accesului la informaţie

(1) Refuzul de a furniza o informaţie, un document oficial va fi făcut în scris, indicîndu-se data întocmirii refuzului, numele persoanei responsabile, motivul refuzului, făcîndu-se în mod obligatoriu trimitere la actul normativ (titlul, numărul, data adoptării, sursa publicaţiei oficiale), pe care se bazează refuzul, precum şi procedura de recurs a refuzului, inclusiv termenul de prescripţie.

(2) Furnizorii de informaţii nu pot fi obligaţi să prezinte probe ale inexistenţei informaţiilor nedocumentate.

Articolul 20. Plăţi pentru furnizarea informaţiilor oficiale

(1) Pentru furnizarea informaţiilor oficiale pot fi percepute, în afara excepţiilor prevăzute de lege, plăţi în mărimile şi conform procedurii stabilite de organele reprezentative, acestea fiind vărsate în bugetul de stat.

(2) Mărimile plăţilor nu vor depăşi mărimile cheltuielilor suportate de către furnizor pentru facerea copiilor, expedierea lor solicitantului şi/sau pentru traducerea, la cererea solicitantului, a informaţiei, documentului.

(3) Plăţile pentru furnizarea informaţiilor analitice, de sinteză sau inedite, executate la comanda solicitantului, se vor stabili conform contractului dintre solicitant şi furnizorul de informaţii.

(4) Vor fi puse, fără plată, la dispoziţia solicitanţilor, informaţiile oficiale care:

a) ating nemijlocit drepturile şi libertăţile solicitantului;

b) sînt expuse oral;

c) sînt solicitate pentru a fi studiate la sediul instituţiei;

d) prin faptul că au fost furnizate, contribuie la sporirea gradului de transparenţă a activităţii instituţiei publice şi corespunde intereselor societăţii.

(5) În cazurile în care informaţia pusă la dispoziţia solicitantului conţine inexactităţi sau date incomplete, instituţia publică este obligată să efectueze rectificările şi completările respective gratuit, cu excepţia cazurilor în care completarea informaţiei implică eforturi şi cheltuieli considerabile care n-au fost prevăzute şi taxate la eliberarea primară a informaţiilor.

(6) Instituţia publică va aduce la cunoştinţa solicitanţilor într-un mod cît mai adecvat şi mai amănunţit posibil modalitatea de calculare a plăţilor pentru furnizarea informaţiei.

Articolul 21. Dispoziţii generale privind apărarea dreptului de acces la informaţie

(1) Persoana care se consideră lezată într-un drept sau interes legitim de către furnizorul de informaţii poate ataca acţiunile acestuia atît pe cale extraju-

diciară, cît şi direct în instanţa de contencios administrativ competentă.

(2) Persoana, de asemenea, se poate adresa pentru apărarea drepturilor şi intereselor sale legitime Avocatului Poporului.

(3) Persoana care se consideră lezată într-un drept sau interes legitim poate ataca orice acţiune sau inacţiune a persoanei responsabile pentru primirea şi examinarea cererilor de acces la informaţii, dar în special cu privire la:

a) refuzul neîntemeiat de a primi şi înregistra cererea;

b) refuzul de a asigura accesul liber şi necondiţionat la registrele publice aflate la dispoziţia furnizorului de informaţii;

c) încălcarea termenelor şi procedurii de soluţionare a cererii de acces la informaţie;

d) neprezentarea sau prezentarea necorespunzătoare a informaţiilor solicitate;

e) refuzul neîntemeiat de a prezenta informaţiile solicitate;

f) atribuirea neîntemeiată a informaţiei la categoria informaţiilor care conţin secrete de stat, secrete comerciale sau la categoria altor informaţii oficiale cu accesibilitate limitată;

g) secretizarea neîntemeiată a unor informaţii;

h) stabilirea plăţii şi mărimii acesteia pentru informaţiile furnizate;

i) cauzarea unor prejudicii materiale şi/sau morale prin acţiunile ilegale ale furnizorului de informaţii.

(4) În cadrul soluţionării litigiilor privind accesul la informaţie, organele competente vor întreprinde măsuri pentru protejarea drepturilor tuturor persoanelor ale căror interese pot fi atinse prin divulgarea informaţiei, inclusiv se va asigura participarea acestora în cadrul procesului în calitate de terţă parte.

(5) Instanţa de judecată, în cadrul examinării litigiilor privind accesul la informaţie, va întreprinde toate măsurile rezonabile şi suficiente de precauţie, inclusiv convocarea şedinţelor închise, pentru a evita divulgarea informaţiilor, accesul limitat la care poate fi îndreptăţit.

Articolul 22. Atacarea pe cale extrajudiciară a acţiunilor furnizorilor de informaţii

(1) În cazul în care persoana consideră că drepturile sau interesele legitime în ceea ce priveşte accesul la informaţii i-au fost lezate, ea poate contesta acţiunile sau inacţiunea furnizorului de informaţii la conducerea acestuia şi/sau la organul ierarhic superior al furnizorului în termen de 30 de zile de la data cînd a aflat sau trebuia să afle despre încălcare.

(2) Conducerea furnizorului de informaţii şi/sau organul ierarhic superior al acestuia va examina contestările solicitanţilor de informaţii în decurs de 5 zile lucrătoare şi va informa în mod obligatoriu petiţionarul despre rezultatele examinării în decurs de 3 zile lucrătoare.

(3) Sesizările, prin care sînt atacate acţiunile sau inacţiunea organizaţiilor care nu au organele lor superioare, sînt adresate direct instanţei de contencios administrativ competente.

Articolul 23. Atacarea pe cale judiciară a acţiunilor furnizorilor de informaţii

(1) În cazul în care persoana care consideră că drepturile sau interesele legitime în ceea ce priveşte accesul la informaţie i-au fost lezate, precum şi în cazul în care nu este satisfăcută de soluţia dată de către conducerea furnizorului de informaţii sau de către organul ierarhic superior al acestuia, ea poate ataca acţiunile sau inacţiunea furnizorului de informaţii direct în instanţa de contencios administrativ competentă.

(2) Sesizarea instanţei de judecată se va efectua în termen de o lună de la data primirii răspunsului de la furnizorul de informaţii sau, în caz dacă nu a primit răspuns, de la data cînd trebuia să-l primească. Dacă solicitantul de informaţii a atacat anterior acţiunile furnizorului de informaţii pe cale extrajudiciară, termenul de o lună curge de la data comunicării răspunsului conducerii furnizorului de informaţii şi/sau organului ierarhic superior al acestuia sau, în caz dacă nu a primit răspuns, de la data cînd trebuia să-l primească.

Articolul 24. Consecinţele prejudicierii dreptului de acces la informaţii

În funcţie de gravitatea efectelor pe care le-a avut refuzul nelegitim al funcţionarului public, responsabil pentru furnizarea informaţiilor oficiale, de a asigura accesul la informaţia solicitată, instanţa de judecată decide aplicarea unor sancţiuni în conformitate cu legislaţia, repararea prejudiciului cauzat prin refuzul nelegitim de a furniza informaţii sau prin alte acţiuni ce prejudiciază dreptul de acces la informaţii, precum şi satisfacerea neîntîrziată a cererii solicitantului.

PARLAMENTUL

LEGE Nr. 1069 din 22-06-2000

cu privire la informatică

Publicat : 05-07-2001 în Monitorul Oficial Nr. 73-74 art. 547

MODIFICAT LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20

Capitolul I

DISPOZIŢII GENERALE

Art. 1. - Prezenta lege stabileşte principalele reguli şi condiţii de activitate în domeniul informaticii în Republica Moldova, drepturile şi obligaţiile statului, ale persoanelor juridice şi fizice în procesul creării, administrării, utilizării şi întreţinerii sistemelor informatice, principiile şi măsurile de asigurare a libertăţii şi protecţiei datelor în sistemele informatice, dreptului de acces la serviciile informatice.

Art. 2. - În sensul prezentei legi, se definesc următoarele noţiuni:

acces neautorizat - acces la informaţii efectuat cu încălcarea regimului de lucru;bancă de date - totalitatea bazelor de date şi produselor program pentru dirijarea lor;bază de date - colecţie de date, organizată conform unei structuri conceptuale, care descrie caracteristicile acestor date şi relaţiile dintre entităţile lor componente, destinată unuia sau mai multor domenii de aplicaţie;

date - fapte, noţiuni, fenomene, evenimente, însuşiri, indici, instrucţiuni etc., reprezentate sub o formă convenţională, adecvată comunicării, interpretării sau prelucrării manuale ori cu mijloace automate;

date publice - date la care accesul public este nelimitat;

date cu caracter personal - date care permit sub orice formă, direct sau indirect, identificarea persoanei fizice la care se referă aceste date;

date nominative - date al căror ansamblu poate duce la identificarea unei persoane, fără a fi totuşi recunoscută, fiecare în parte, ca identificator;

document electronic - produs informatic prin care se adevereşte sau se preconizează un fapt, se confirmă un drept, se recunoaşte o obligaţie, se identifică o persoană juridică sau fizică etc.;

echipamente (hardware) - mijloace tehnice destinate sistemelor de calcula-

toare;

informatică - domeniu de activitate care include prelucrarea şi transportul datelor cu ajutorul sistemelor automatizate de calcul şi mijloacelor de telecomunicaţie;

informatizare - ansamblu organizat de acţiuni destinate creării, implementării, întreţinerii şi perfecţionării sistemelor automatizate de calcul şi transport de date în procesul de colectare, stocare, prelucrare şi difuzare a informaţiei;

flux al datelor - transport de date între constante sau fişiere, efectuat ca urmare a execuţiei unor instrucţiuni, proceduri, module de program sau programe;

operator informatic - persoană juridică capabilă să presteze o gamă largă de servicii informatice, în condiţii de calitate şi securitate, la nivelul cerinţelor internaţionale;

produs informatic - ansamblu de date şi programe obţinute în urma rulării unor programe sau pachete de programe;

produse program (software) - totalitate sau o parte a programelor, procedurilor, regulilor şi documentelor asociate ale unui sistem de prelucrare a informaţiei;

program (program pe calculator) - secvenţă de declaraţii şi instrucţiuni ale unui limbaj de programare, lansată într-un mediu operaţional al calculatorului, pentru îndeplinirea anumitelor funcţii ori soluţionarea unor probleme;

protecţia datelor - totalitatea procedurilor organizaţional-tehnice şi actelor normative utilizate pentru a se evita cauzarea oricăror pagube intereselor proprietarilor de date, sistemelor informatice, precum şi utilizatorilor de informaţii;

resursă informaţională - orice element al unui sistem informaţional, necesar pentru executarea operaţiilor solicitate;

reţea informatică (reţea de calculatoare) - ansamblu de noduri de prelucrare a datelor interconectate în scopul transportului de date;

reţea publică de transport de date - reţea informatică ce se utilizează în domeniul public;
securitatea datelor - atribut al datelor ce caracterizează siguranţa lor faţă de evenimente ce le-ar putea afecta integralitatea;

serviciu informatic - serviciu oferit pe piaţă privind întreţinerea produselor program, echipamentelor şi sistemelor informatice;

serviciu informatic public - serviciu informatic prestat prin intermediul reţelei publice de transport de date;

sistem informatic - ansamblu de programe şi echipamente care asigură pre-

lucrarea automată a datelor;

sistem informaţional - sistem de prelucrare a informaţiei, împreună cu resursele organizaţionale asociate, cum ar fi resursele umane şi tehnice, care furnizează şi distribuie informaţia;

tehnologiile informaţiei - tehnologii specifice informaticii, precum şi acelei părţi a comunicaţiei aferente traficului informatic în reţelele informatice;

trafic informatic - circulaţie a datelor şi programelor între doi sau mai mulţi utilizatori.

Art. 3. - (1) Accesul oricărei persoane juridice şi fizice la serviciile informatice publice şi la informaţiile ce se conţin în sistemele informatice este asigurat în conformitate cu prevederile respective ale Constituţiei, prezentei legi şi altor acte legislative.

(2) Sistemele şi reţelele informatice, precum şi resursele informaţionale pot aparţine persoanelor juridice şi fizice cu titlu de proprietate privată sau publică.

Art. 4. - (1) Protecţia datelor în cadrul sistemelor şi reţelelor informatice este asigurată în conformitate cu prevederile respective ale Constituţiei, prezentei legi, altor acte normative.

(2) Persoanele care activează în cadrul sistemelor şi reţelelor informatice sînt obligate să asigure protecţia datelor.

(3) Se interzice accesul şi conectarea neautorizate la sistemele şi reţelele informatice.

(4) Utilizarea mijloacelor informatice în condiţii nediscriminatorii este garantată pe întreg teritoriul ţării.

Art. 5. – (1) Ministerul Economiei și Infrastructurii este organul central de specialitate care elaborează documentele de politici şi actele normative în domeniul informaticii şi al tehnologiilor informației.

(2) Funcțiile şi atribuțiile Ministerului Economiei şi Infrastructurii în domeniul informaticii şi al tehnologiilor informației sunt stabilite de către Guvern.

(3) Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei este autoritatea administrativă centrală care reglementează activitatea în domeniul informaticii şi al tehnologiilor informației conform legislației.

(4) Funcțiile şi atribuțiile de bază ale Agenţiei Naţionale pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei privind reglementarea activității în domeniul informaticii şi al tehnologiilor informației sunt stabilite de Legea comunicațiilor electronice nr. 241/2007.

[Art.5 în redacţia LP135 din 16.07.20, MO199-204/07.08.20 art.410; în

vigoare 07.08.20]

Art. 6. - (1) Relaţiile din domeniul informaticii, nespecificate în prezenta lege, se reglementează de alte acte normative.

(2) Pentru Republica Moldova, relaţiile internaţionale în domeniul informaticii se reglementează prin convenţii şi acorduri internaţionale la care aceasta este parte. În cazul în care convenţiile şi acordurile internaţionale conţin alte norme decît cele prevăzute de legislaţia Republicii Moldova cu privire la informatică, se aplică prevederile convenţiilor şi acordurilor internaţionale.

[Capitolul II abrogat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Capitolul III

ACCESUL LA INFORMAŢIE ŞI SERVICIILE INFORMATICE

Art. 13. - (1) Circulaţia datelor pe teritoriul Republicii Moldova este liberă pentru toţi participanţii la traficul informatic.

(2) Fluxurile transfrontaliere ale datelor supuse unei prelucrări automatizate sau ale celor colectate în vederea unei asemenea prelucrări sînt permise în măsura în care nu lezează drepturile personale, libertăţile şi îndatoririle cetăţeneşti, nu afectează secretul şi confidenţialitatea informaţiei, cerute de apărarea ordinii de drept în stat şi societate.

Art. 14. - (1) Persoanele care creează şi furnizează produse informatice sau care prestează servicii informatice sînt obligate:

a) să asigure şi să garanteze utilizatorilor de produse şi servicii că acestea nu sunt de natură să afecteze drepturile omului;

b) să prevadă, în produsul sau în serviciul prestat, modalităţile de apărare a drepturilor utilizatorului, a libertăţilor individuale;

c) să repare, total sau parţial, după caz, prejudiciul adus persoanelor prin nerespectarea cerinţelor prevăzute la lit. a) şi b).

(2) Pentru nerespectarea prevederilor indicate la alin.(1) lit.a) şi b), titularii de date şi de reţele informatice poartă răspundere conform legislaţiei.

Art. 15. - (1) Sînt considerate informaţii de categorie specială şi nu pot face obiectul deţinerii şi prelucrării în baze de date datele cu caracter personal privind originea rasială sau etnică, opiniile politice, convingerile religioase sau alte convingeri, datele referitoare la sănătate sau viaţa sexuală a persoanei, precum şi cele referitoare la antecedentele penale. Astfel de date pot fi prelucrate şi deţinute de organe special constituite şi autorizate pentru aceasta şi care sînt

obligate să ia măsuri şi garanţii corespunzătoare de protecţie şi nedivulgare.

(2) Sînt excluse de la deţinerea şi prelucrarea în baze de date datele ce constituie informaţii oficiale cu accesibilitate limitată ale altor titulari care au stabilit caracterul lor, cu excepţia celor autorizate sau obligatorii pentru păstrare potrivit legislaţiei.

(3) Datele de interes public, cu excepţia celor prevăzute la alin.(1) şi (2), pot fi prelucrate şi deţinute liber, fără restricţii şi obligaţii de natură morală sau materială din partea titularilor de date, în cadrul obiectului lor de activitate.

Art. 16. - (1) Orice persoană este în drept să deţină date, programe şi echipamente, precum şi să prelucreze date şi programe, cu obţinerea unor produse informatice pentru uz propriu, dacă aceasta nu contravine prevederilor prezentei legi.

(2) În măsura în care activităţile prevăzute la alin.(1) depăşesc sfera activităţilor admise prin accesul la bazele de date ale altor titulari, acestea, în mod obligatoriu, urmează a fi aduse în conformitate cu dispoziţiile ce reglementează fluxul de date.

Art. 17. - Transferul de date cu caracter personal către utilizatori din alte ţări nu poate avea loc decît dacă aceştia asigură un nivel de protecţie a datelor conform legislaţiei şi reglementărilor în vigoare.

Art. 18. - Datele aflate în trafic prin orice mijloace tehnice şi/sau suporturi materiale se bucură, din punct de vedere juridic, de protecţie similară celei asigurate conform legislaţiei cu privire la secretul corespondenţei şi convorbirilor telefonice.

Art. 19. - (1) Pentru prelucrarea datelor se definesc, în prealabil sau cel mai tîrziu în momentul colectării acestora, scopurile în care se întreprinde această activitate.

(2) Orice prelucrare a datelor şi utilizare ulterioară a acestora trebuie să se efectueze exclusiv în scopurile stabilite şi compatibile cu ele.

(3) Prevederile alin.(1) şi (2) nu sînt aplicabile datelor şi prelucrărilor de natură statistică sau previzională cu caracter general şi local, precum şi celor recunoscute legal ca publice.

Art. 20. - (1) Persoanele juridice şi fizice au dreptul să obţină de la titularii bazelor de date, direct sau pe alte căi de acces, confirmarea că aceştia deţin sau nu date care se referă la persoana respectivă.

(2) Dreptul prevăzut la alin.(1) nu se extinde asupra activităţilor de informatică legale ce constituie informaţie oficială cu accesibilitate limitată, precum şi asupra datelor rezultate din asemenea activităţi.

Art. 21. - (1) Persoanele fizice au dreptul să obţină informaţiile cu caracter

personal, care se referă la ele, conţinute în bazele de date. Titularul de date trebuie să dea răspunsul la aceste solicitări în termen legal, sub o formă inteligibilă şi fără pretenţii materiale.

(2) Persoanele lezate prin înscrierea într-o bază de date a datelor cu caracter personal care se referă la ele le pot contesta şi, în măsura în care această contestare este întemeiată, titularul de date este obligat să le şteargă, modifice, completeze sau corecteze.

(3) Persoanele fizice au dreptul să fie informate asupra motivelor pentru care demersurile lor depuse în conformitate cu alin.(1) şi (2) au fost respinse, precum şi dreptul de a contesta motivele respingerii.

Art. 22. - Persoanele juridice şi fizice au drept de acces la datele publice, precum şi la metodologia de definire a indicatorilor utilizaţi în colectarea şi prelucrarea informaţiei publice, a clasificatoarelor şi nomenclatoarelor utilizate.

Art. 23. - (1) Informaţiile atribuite la secret de stat, la care accesul este limitat, precum şi modul de acces, de utilizare, de acumulare, de protejare a acestora şi lista persoanelor care au acces la aceste informaţii sînt reglementate de legislaţia cu privire la secretul de stat.

(2) Nu poate fi limitat accesul la datele:

a) care stabilesc statutul juridic al persoanelor juridice, drepturile, libertăţile şi obligaţiile persoanelor fizice şi procedurile realizării acestor drepturi şi libertăţi;

b) cu privire la situaţiile excepţionale ecologice, meteorologice, sanitaro-epidemiologice şi altă informaţie necesară pentru asigurarea funcţionării obiectelor de producţie, securităţii populaţiei;

c) care reprezintă surse de cunoştinţe acumulate în sistemele informatice din sferele învăţămîntului, ocrotirii sănătăţii, ştiinţei, culturii şi jurisprudenţei.

Capitolul IV
PROTECŢIA ŞI SECURITATEA DATELOR

Art. 24. - Autorităţile administraţiei publice care au colectat informaţia sînt obligate să o furnizeze, la solicitare, celorlalte autorităţi ale administraţiei publice, în conformitate cu legislaţia.

Art. 25. - Bazele de date se organizează conform criteriului calităţii şi securităţii datelor ce le conţin, indiferent de faptul că ele sînt ţinute pentru păstrare şi consultare internă sau că din acestea se furnizează produse informatice transmise unor terţi, inclusiv pe cale neinformatică.

Art. 26. - (1) În aplicarea art. 25, la bazele de date din domeniul public se desemnează responsabili pentru prelucrarea datelor.

(2) Titularii de date care nu aparţin domeniului public, dar care stochează, prelucrează, difuzează sau utilizează date ce pot intra în categoria celor cu caracter personal sau a datelor nominative trebuie să desemneze responsabili pentru prelucrarea datelor.

Art. 27. - Titularul bazelor de date protejează, prin măsuri adecvate, datele colectate, echipamentele şi produsele program utilizate pentru administrarea acestora, asigurînd securitatea datelor împotriva riscurilor de pierdere, distrugere, precum şi împotriva folosirii neautorizate sau divulgării.

Art. 28. - (1) Persoanele care activează în cadrul sistemelor şi reţelelor informatice sînt obligate să asigure protecţia şi confidenţialitatea datelor, cu excepţia celor care sînt determinate ca date publice.

(2) În scopul asigurării protecţiei datelor şi evitării infracţiunilor ce ţin de domeniul informaticii, se interzice:

a) elaborarea şi instalarea în reţelele informatice a produselor program ce pot modifica, deteriora, distruge datele, produsele program şi echipamentele;

b) pătrunderea neautorizată în sistemele şi reţelele informatice publice sau private pentru a capta, memora, prelucra sau difuza date şi programe ori pentru a modifica, deteriora, distruge date, programe şi echipamente;

c) deturnarea datelor, perturbarea programelor ori falsificarea mesajelor sau transmiterea datelor eronate în scopul deranjamentului fluxului de date sau creării unei stări de neîncredere între participanţii la circuitul informatic;

d) pătrunderea neautorizată şi cu intenţie în sistemele şi reţelele informatice publice sau private, chiar neurmată de ascultarea, înregistrarea sau utilizarea în interese personale ori în interesele altor persoane a datelor culese, precum şi pentru obţinerea unui alt folos.

(3) În scopul asigurării securităţii naţionale, organele abilitate au drept de acces la resursele informaţionale din sistemele informatice publice sau private. În procesele penale, organele menţionate pot, în baza mandatului emis de procuror, intercepta reţelele informatice, utilizînd aparatajul tehnic al proprietarului sistemului informatic.

Capitolul V
DREPTUL DE PROPRIETATE ASUPRA PRODUSELOR INFORMATICE

Art. 29. - (1) Obiecte ale dreptului de proprietate în domeniul informaticii pot fi:

a) resursele informaţionale şi datele, cum ar fi: băncile de date, bazele de date, fişierele textuale, grafice şi audiovizuale, precum şi părţi de sine stătătoare ale acestora;

b) sistemele informatice.

(2) Subiecte ale dreptului de proprietate în domeniul informaticii pot fi statul - prin autorităţile administraţiei publice, precum şi persoanele juridice şi fizice.

(3) Obiectele dreptului de proprietate în domeniul informaticii, create în urma finanţării de la bugetul de stat, se consideră bunuri publice. Bunul public poate fi transmis şi utilizat în temeiul contractului încheiat cu autoritatea abilitată de Guvern.

(4) Proprietarul produselor informatice are dreptul de a autoriza persoane care să posede, utilizeze şi/sau să administreze aceste produse, fiind în drept să efectueze orice operaţiune legală cu acestea şi în privinţa acestora.

Art. 30. - (1) Dreptul de proprietate asupra produsului informatic îl obţin:

a) creatorul - în urma creării produsului informatic cu forţe proprii şi pe cont propriu;

b) persoana care a făcut comandă de creare a produsului informatic şi a finanţat toate lucrările aferente creării acestuia - în baza contractului încheiat cu creatorul produsului informatic;

c) persoana juridică sau fizică ce intenţionează să folosească programul sau baza de date - în baza contractului încheiat cu proprietarul produsului informatic;

d) moştenitorii şi alţi succesori de drepturi ai proprietarului - conform legislaţiei.

(2) Dreptul de proprietate asupra datelor noi, obţinute în procesul prelucrărilor din cadrul sistemului informatic, se stipulează în contractul dintre proprietarul resurselor informaţionale şi al datelor şi proprietarul sistemului informatic. Dacă această stipulare lipseşte în contractul dintre părţi, atunci dreptul de proprietate asupra acestor date aparţine proprietarului sistemului informatic.

(3) Dreptul de proprietate asupra produselor informatice se protejează de către legislaţia cu privire la proprietate.

[Capitolul VI abrogat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Capitolul VII

RĂSPUNDERI

Art. 37. - Persoanele juridice şi fizice care încalcă prevederile prezentei legi poartă răspundere administrativă, materială sau penală, după caz, conform legislaţiei.

PARLAMENTUL

LEGE Nr. 467 din 21-11-2003

cu privire la informatizare şi la resursele informaţionale de stat

Publicat : 01-01-2004 în Monitorul Oficial Nr. 6-12 art. 44

MODIFICAT LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20

Capitolul I

DISPOZIŢII GENERALE

Articolul 1. Obiectul reglementării

(1) Prezenta lege stabileşte regulile de bază şi condiţiile de activitate în domeniul creării şi dezvoltării infrastructurii informaţionale naţionale ca mediu de funcţionare al societăţii informaţionale din Republica Moldova, reglementează raporturile juridice care apar în procesul de creare, formare şi utilizare a resurselor informaţionale automatizate de stat, a tehnologiilor, sistemelor şi reţelelor informaţionale.

(2) Sub incidenţa prezentei legi nu cad raporturile care apar la crearea şi funcţionarea mijloacelor de informare în masă, resurselor informaţionale nestatale, la prelucrarea informaţiei nedocumentate.

Articolul 2. Cadrul juridic

(1) Legislaţia în domeniul informatizării include Constituţia Republicii Moldova, tratatele internaţionale la care Republica Moldova este parte, prezenta lege, alte acte normative ce reglementează raporturile aferente informatizării şi resurselor informaţionale de stat.

(2) În cazul neconcordanţei prezentei legi cu tratatele internaţionale la care Republica Moldova este parte, se aplică normele tratatelor internaţionale.

Articolul 3. Noţiuni principale

În sensul prezentei legi, următoarele noţiuni principale semnifică:

bază de date - totalitate de date, organizate conform unei structuri conceptuale, ce descriu caracteristicile principale şi raporturile dintre esenţe, destinată unui domeniu sau mai multor domenii de aplicare;

bancă de date – sistem tehnico-informaţional ce include una sau mai multe baze de date şi un sistem de dirijare a acestor baze;

complex de mijloace tehnice de program - totalitate de mijloace tehnice şi de mijloace de program care asigură realizarea proceselor informaţionale;

date - informaţie prezentată într-o anumită formă care permite a o comunica, comenta şi prelucra;

date personale - date despre o persoană fizică ce permit identificarea ei directă sau indirectă;

document – suport pe care este fixată informația și care posedă atribute ce permit identificarea acestuia;

[Art.3 noțiunea introdusă prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

document electronic – astfel cum este definit la art. 2 din Legea nr. 91/2014 privind semnătura electronică și documentul electronic;

[Art.3 noțiunea în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

domenul naţional de nivel superior „.md” - codul Republicii Moldova, atribuit de Corporaţia de Atribuire a Numelor şi Numerelor în Internet (ICANN), în conformitate cu standardul internaţional ISO-3166, în calitate de nume de domen de nivel superior pentru identificarea ţării în reţeaua globală Internet;

informatizare - proces organizatoric social-economic şi tehnico-ştiinţific de creare a unor condiţii optime pentru satisfacerea necesităţilor informaţionale şi realizarea drepturilor cetăţenilor, autorităților publice, instituțiilor publice şi persoanelor juridice în baza formării şi utilizării resurselor informaţionale;

[Art.3 noțiunea modificată prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

informaţie - cunoştinţe despre persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situaţii şi idei;

informaţie documentată - informaţie, fixată pe un suport informaţional, care posedă atribute ce permit identificarea ei;

protecția informației – totalitatea activităților privind prevenirea accesului neautorizat la informația documentată protejată;

[Art.3 noțiunea introdusă prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

infrastructură informaţională - totalitate de centre informaţionale de calcul, de bănci de date şi de cunoştinţe din sistemul automatizat integrat de telecomunicaţii şi de organizare care asigură utilizatorilor condiţii generale de

acces la informaţia păstrată;

model spaţial al localităţii - totalitate de date spaţiale şi de date descriptive, prezentate în formă digitală, destinate reproducerii imaginilor volumetrice ale localităţii, obiectivelor topografice, şi de date suplimentare conform condiţiilor stabilite în regimul timpului real;

posesor de resurse şi sisteme informaţionale, de tehnologii şi mijloace de asigurare a

acestora - persoană fizică, persoană juridică sau statul, avînd drept de posesiune şi folosinţă asupra resurselor şi sistemelor informaţionale, tehnologiilor şi mijloacelor de asigurare a acestora, în condiţiile stabilite de titularul drepturilor respective;

proces informaţional - proces de colectare, prelucrare, acumulare, păstrare, actualizare şi furnizare către utilizator a informaţiei documentate;

produs informaţional - rezultat al procesului de prelucrare a informaţiei cu ajutorul sistemelor informaţionale automatizate, destinat satisfacerii necesităţilor utilizatorului;

proprietar al resurselor şi sistemelor informaţionale, al tehnologiilor şi mijloacelor de asigurare a acestora - persoană fizică, persoană juridică sau statul care exercită integral dreptul de posesiune, folosinţă şi dispoziţie asupra resurselor şi sistemelor informaţionale, tehnologiilor şi mijloacelor de asigurare a acestora;

resursă informaţională - totalitate de informaţii documentate în sistemele informaţionale automatizate, organizată în conformitate cu cerinţele stabilite şi cu legislaţia în vigoare;

[Art.3 noţiunea „reţea de comunicaţii" exclusă prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

serviciu informaţional - activitate de furnizare a produselor informaţionale;

sistem informaţional - totalitate de resurse şi tehnologii informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie;

administrarea sistemului informațional – activitate care include: administrarea tehnică a sistemului informațional; gestiunea accesului la resursa informațională; monitorizarea acțiunilor utilizatorilor, a accesării și a actualizării datelor, a modului de furnizare a informațiilor în resursa informațională, a respectării cerințelor de securitate privind accesul la resursa informațională și a regulilor de exploatare a sistemului informațional; instruirea tuturor categoriilor de utilizatori ai sistemului informațional și a registratorilor resursei informaționale privind utilizarea sistemului informațional; implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de protecție a informației și a

securității datelor cu caracter personal;

[Art.3 noțiunea introdusă prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

mentenanța sistemului informațional – activitate care include: asigurarea funcționalității și a securității complexului de mijloace tehnice și de program; actualizarea versiunii sistemului informațional; întreținerea sistemului și resursei informaționale; restabilirea funcționalității sistemului informațional, în cazul apariției defecțiunilor; asigurarea suportului metodologic și practic pentru utilizatori;

[Art.3 noțiunea introdusă prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

dezvoltarea sistemului informațional – crearea și implementarea unor noi module funcționale și/sau modificarea modulelor existente ale unui sistem informațional, precum și reingineria sistemului informațional;

[Art.3 noțiunea introdusă prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

securitate cibernetică – stare de normalitate a sistemului și resursei informaționale, rezultată în urma aplicării unui ansamblu de măsuri prin care este asigurată autenticitatea, integritatea, confidențialitatea, disponibilitatea și nonrepudierea datelor;

[Art.3 noțiunea introdusă prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

subiectul datelor personale - persoană fizică purtător de date personale;

suport informațional - suport material ale cărui calități fizice permit imprimarea, păstrarea și prelucrarea informației documentate;

tehnologie informațională - totalitate de metode, procedee și mijloace de prelucrare și transmitere a informației și regulile de aplicare a acesteia;

unitate de drept - persoană fizică acționînd în bază de licență ori patentă de întreprinzător, persoană juridică sau o totalitate a unor astfel de persoane cu orice formă juridică de organizare, înregistrate în modul stabilit de lege;

utilizator de informație – persoană fizică sau persoană juridică ce efectuează acțiuni de prezentare, primire, păstrare și alte acțiuni de utilizare a informației documentate în sistem informațional automatizat.

Articolul 4. Obiectul dreptului de proprietate al statului în sfera informatizării

Sînt obiect al dreptului de proprietate al statului în sfera informatizării:

a) informația documentată;

b) resursele informaţionale, inclusiv domenul naţional de nivel superior „.md”;

c) tehnologiile informaţionale;

d) produsele de program şi mijloacele tehnice;

e) sistemele şi reţelele informaţionale.

Articolul 5. Subiectul dreptului de proprietate al statului în sfera informatizării

Dreptul de proprietate, inclusiv intelectuală, al statului asupra resurselor informaţionale de stat este dobîndit şi exercitat prin intermediul autorităţilor şi instituţiilor publice.

[Art.5 modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 6. Dreptul de proprietate în sfera informatizării

(1) Apariţia, modificarea şi încetarea dreptului de proprietate în sfera informatizării sînt reglementate de legislaţie.

(2) Dreptul de proprietate, inclusiv intelectuală, asupra obiectelor informatizării poate aparţine persoanelor fizice, persoanelor juridice sau statului în temeiul legii, al titlului de proprietate şi/sau în bază de contract.

(3) Obiectele dreptului de proprietate în sfera informatizării se consideră, în condiţiile legii, mărfuri (produse) şi fac parte din patrimoniul proprietarului sau posesorului lor.

Articolul 7. Subiectele raporturilor juridice în sfera informatizării

(1) Sînt subiecte ale raporturilor juridice în sfera informatizării statul, în persoana autorităţilor şi instituţiilor publice, persoanele fizice şi juridice, precum şi organizaţiile internaţionale, alte state, persoanele fizice şi persoanele juridice străine, apatrizii.

[Art.7 al.(1) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(2) Subiecţi ai raporturilor juridice în domeniul creării, administrării, mentenanţei, dezvoltării şi utilizării sistemelor informaţionale de stat sunt:

a) proprietarul sistemului informaţional;

b) posesorul sistemului informaţional;

c) deţinătorul sistemului informaţional;

d) administratorul tehnic al sistemului informaţional;

e) utilizatorii sistemului informaţional.

[Art.7 al.(2) în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 7[1]. Proprietarul sistemelor informaționale de stat

(1) Proprietar al sistemelor informaționale de stat este statul.

(2) Proprietarul stabilește posesorii, deținătorii, administratorii tehnici și utilizatorii sistemelor informaționale de stat.

[Art.7[1] *introdus prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]*

Articolul 7[2]. Posesorii sistemelor informaționale de stat

(1) Posesori ai sistemelor informaționale de stat sunt autoritățile și instituțiile publice.

(2) Posesorul asigură condițiile juridice, financiare şi organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea sistemului informațional de stat.

(3) Posesorul sistemului informațional de stat poate exercita atribuțiile deținătorului, administratorului tehnic și utilizatorului sistemului informațional de stat.

[Art.7[2] *introdus prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]*

Articolul 7[3]. Deținătorii sistemelor informaționale de stat

(1) Deţinători ai sistemelor informaţionale de stat sunt autoritățile publice, instituţiile publice şi alte entități de stat.

(2) Deţinătorul sistemului informaţional de stat asigură crearea, administrarea, mentenanța şi dezvoltarea sistemului informaţional.

(3) Deținătorul sistemului informațional de stat poate exercita atribuțiile administratorului tehnic şi ale utilizatorului sistemului informațional de stat.

[Art.7[3] *introdus prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]*

Articolul 7[4]. Administratorii tehnici ai sistemelor informaționale de stat

(1) Administratori tehnici ai sistemelor informaționale de stat sunt autoritățile publice, instituţiile publice şi alte entități de stat.

(2) Administratorul tehnic al sistemului informațional de stat asigură:

a) administrarea tehnică a sistemului informațional de stat;

b) mentenanța sistemului informațional de stat;

c) dezvoltarea sistemului informațional de stat;

d) implementarea cerințelor de securitate stabilite de actele normative în domeniu.

[Art.7[4] *introdus prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]*

Articolul 7[5]. Utilizatorii sistemelor informaționale de stat

Utilizatori ai sistemelor informaționale de stat sunt persoanele fizice și/sau persoanele juridice de drept public sau privat.

[Art.7[5] *introdus prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]*

Articolul 7[6]. Documentele sistemelor și resurselor informaționale de stat

(1) Documentarea sistemelor și resurselor informaționale de stat este obligatorie.

(2) Documentele sistemelor și resurselor informaționale de stat sunt:

a) conceptul sistemului informațional, în care să fie definite: spațiul funcțional, structura organizatorică, spațiul informațional, spațiul tehnologic, securitatea sistemului informațional și protecția informației;

b) caietul de sarcini al sistemului informațional, care include cerințele funcționale și tehnice în conformitate cu care se creează sistemul informațional;

c) regulamentul resursei informaționale, care să cuprindă: reglementări privind drepturile și obligațiile subiecților raporturilor juridice aferente creării și ținerii resursei informaționale; modalitatea de ținere a resursei informaționale; procedura de înregistrare, modificare, completare și radiere a datelor; procedura de interacțiune cu furnizorii de date; măsuri privind asigurarea securității resursei informaționale.

(3) Documentele sistemelor informaționale de stat sunt elaborate în conformitate cu cadrul normativ metodologic privind crearea, administrarea, mentenanța, dezvoltarea și scoaterea din exploatare a sistemelor informaționale de stat, aprobat de către Guvern.

[Art.7[6] *introdus prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]*

Capitolul II

INFORMAŢIA DOCUMENTATĂ

Articolul 8. Documentarea informaţiei

(1) Documentarea informaţiei este o condiţie obligatorie pentru includerea informaţiei în resursele informaţionale de stat. Documentarea informaţiei se efectuează de autorităţile şi instituţiile publice abilitate.

[Art.8 al.(1) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(2) Informaţia documentată se întocmeşte, se selectează, se prelucrează, se sistematizează şi se asigură cu atributele respective în funcţie de sursa, forma, destinaţia şi suportul ei.

(3) Lista informaţiei documentate, care se prezintă în mod obligatoriu, şi lista organelor şi organizaţiilor responsabile de colectarea şi prelucrarea resurselor informaţionale de stat se aprobă de Guvern.

(4) Informaţia documentată ca obiect al dreptului de proprietate apare în formă de document aparte ori de totalitate de documente, în formă de document electronic sau de document pe suport informaţional.

(5) Documentul ce conţine informaţie prelucrată în sistemul informaţional automatizat dobîndeşte putere juridică după autentificarea lui, în modul stabilit, inclusiv prin semnătură electronică avansată calificată, de către persoana cu funcţie de răspundere abilitată.

[Art.8 al.(5) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(6) Regimul juridic de utilizare a semnăturii electronice se stabileşte de lege.

[Art.8 al.(6) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

[Art.8 al.(7) abrogat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 9. Datele cu caracter personal

Colectarea, prelucrarea, stocarea şi utilizarea datelor cu caracter personal în cadrul sistemelor şi resurselor informaţionale de stat se realizează în conformitate cu prevederile legislaţiei în domeniul protecţiei datelor cu caracter personal.

[Art.9 în redacţia LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 10. Securitatea sistemelor şi resurselor informaţionale de stat

(1) Securitatea, inclusiv securitatea cibernetică, a sistemelor şi resurselor in-

formaționale de stat este asigurată de către autoritățile publice, instituţiile publice şi alte entități de stat, în limita competențelor acestora și în conformitate cu reglementările stabilite de către Guvern.

(2) Datele din cadrul sistemelor şi resurselor informaționale de stat sunt protejate împotriva accesării și/sau utilizării neautorizate.

[Art.10 în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Capitolul III

RESURSELE INFORMAŢIONALE DE IMPORTANŢĂ STATALĂ

Articolul 11. Resursele informaţionale de stat

(1) Resursele informaţionale de stat constituie un complex integrat al resurselor informaţionale reprezentate sub formă de bănci de date a căror creare şi utilizare ţin de competenţa autorităților și instituțiilor publice.

[Art.11 al.(1) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(2) Destinaţia, componenţa, modul de formare, gestionare şi păstrare a resurselor informaţionale de stat sînt stabilite de prezenta lege şi de alte acte normative.

(3) Resursele informaţionale de stat se divizează în resurse informaţionale de bază, departamentale şi teritoriale.

(4) Domenul naţional de nivel superior „.md” în reţeaua globală Internet se consideră proprietate a statului şi nu poate fi obiect al vînzării sau închirierii.

(5) Unele resurse informaţionale de stat pot fi declarate patrimoniu naţional al Republicii Moldova. Atribuirea resurselor informaţionale concrete la patrimoniul naţional şi determinarea regimului lor juridic se stabilesc prin lege.

Articolul 12. Resursele informaţionale de bază

Resursele informaţionale de bază se constituie din:

a) Registrul de stat al populaţiei;

b) Registrul de stat al unităţilor de drept.

[Art.12 litc.c) abrogată prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 13. Registrul de stat al populaţiei

(1) Registrul de stat al populaţiei este un sistem unic integrat de evidenţă automatizată a cetăţenilor Republicii Moldova, a cetăţenilor străini şi a apatrizilor domiciliaţi permanent sau aflaţi temporar pe teritoriul ţării, precum şi a cetăţe-

nilor Republicii Moldova plecaţi peste hotare pentru a se stabili permanent sau temporar pe un termen mai mare de 3 luni.

(2) Registrul de stat al populaţiei este destinat colectării, stocării, actualizării şi analizei informaţiei privind persoanele fizice, inclusiv a datelor personale ale acestora, urmând ca informaţia respectivă să fie furnizată autorităţilor şi instituţiilor publice, persoanelor fizice şi persoanelor juridice.

[Art.13 al.(2) în redacţia LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 14. Registrul de stat al unităţilor de drept

(l) Registrul de stat al unităţilor de drept este un sistem unic integrat de evidenţă automatizată a unităţilor de drept înregistrate în Republica Moldova în modul stabilit.

(2) Registrul de stat al unităţilor de drept este destinat colectării, stocării, prelucrării, actualizării şi analizei datelor despre unităţile de drept, această informaţie urmînd să fie prezentată autorităţilor administraţiei publice, persoanelor fizice şi persoanelor juridice.

[Art.15 abrogat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 16. Resursele informaţionale departamentale

(1) Resursele informaţionale departamentale se formează şi se utilizează de către autorităţile şi instituţiile publice, ai căror posesori sînt, şi conţin informaţia necesară executării funcţiunilor lor, cu excepţia datelor ce urmează a fi incluse în resursele informaţionale de bază.

[Art.16 al.(1) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(2) Resursele informaţionale departamentale trebuie să fie interoperabile cu resursele informaţionale de bază, departamentale şi teritoriale respective.

[Art.16 al.(2) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 17. Resursele informaţionale teritoriale

(1) Resursele informaţionale teritoriale se formează şi se utilizează de către autorităţile administraţiei publice locale, ai căror posesori sînt, şi conţin date despre toate tipurile de obiective geografice, naturale şi artificiale, inclusiv despre potenţialul resurselor din teritoriile administrate.

(2) Resursele informaţionale teritoriale trebuie să fie compatibile informaţional-tehnologic cu resursele informaţionale de bază şi cu cele departamentale respective.

Capitolul IV

TEHNOLOGIILE, SISTEMELE ŞI REŢELELE INFORMAŢIONALE

Articolul 18. Crearea tehnologiilor, sistemelor şi reţelelor informaţionale

(1) Autorităţile şi instituțiile publice, persoanele fizice şi persoanele juridice au dreptul să creeze, în limita competenţelor şi în conformitate cu legislaţia, tehnologii, sisteme şi reţele informaţionale în scopul asigurării activităţii proprii şi al prestării de servicii.

(2) Sistemele informaționale care conțin date despre persoanele fizice şi persoanele juridice se creează de către autoritățile şi instituțiile publice, în limita competențelor.

[Art.18 în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 19. Evaluarea conformității sistemelor informaționale de stat

Evaluarea conformității sistemelor informaționale de stat prin prisma corespunderii acestora documentelor prevăzute la art. 7^6 se efectuează de către instituția publică Agenția de Guvernare Electronică, în conformitate cu cadrul normativ metodologic aprobat de către Guvern.

[Art.19 în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Capitolul V

ATRIBUŢIILE AUTORITĂŢILOR ŞI INSTITUȚIILOR PUBLICE ÎN SFERA FORMĂRII ŞI UTILIZĂRII RESURSELOR INFORMAŢIONALE DE STAT ŞI A INFORMATIZĂRII

[Capitolul V denumirea în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 21. Politica informaţională de stat

(1) Politica informaţională de stat este orientată spre crearea condiţiilor juridice, economice, organizatorice şi de altă natură, necesare asigurării unei dezvoltări armonioase a societăţii şi a statului.

(2) Politica privind resursele informaționale de stat este elaborată de Ministerul Economiei și Infrastructurii şi aprobată de Guvern.

Articolul 22. Atribuţiile Guvernului

În vederea executării prezentei legi, Guvernul:

a) aprobă documente de politici şi reglementări în domeniul informatizării, al sistemelor şi resurselor informaţionale de stat;

b) stabileşte împuternicirile autorităţilor şi instituţiilor publice în domeniul creării, administrării, mentenanţei, dezvoltării şi utilizării sistemelor şi resurselor informaţionale de stat;

c) aprobă crearea sistemelor şi resurselor informaţionale de stat;

d) aprobă conceptele sistemelor informaţionale de stat şi regulamentele resurselor informaţionale de stat;

e) aprobă regulile şi modul de găzduire a sistemelor informaţionale de stat.

[Art.22 în redacţia LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 23. Competenţele de bază ale autorităţilor şi instituţiilor publice în domeniul sistemelor şi resurselor informaţionale de stat

(1) Ministerul Economiei şi Infrastructurii este organul central de specialitate care elaborează documentele de politici şi actele normative în domeniul informatizării, al sistemelor şi resurselor informaţionale de stat, precum şi exercită şi alte atribuţii în conformitate cu regulamentul acestuia aprobat de către Guvern.

(2) Instituţia publică Agenţia de Guvernare Electronică elaborează cadrul metodologic pentru administrarea, mentenanţa, dezvoltarea şi scoaterea din exploatare a sistemelor informaţionale de stat, coordonează şi monitorizează crearea, administrarea şi dezvoltarea sistemelor informaţionale de stat, asigură evidenţa acestora, efectuează auditul de securitate cibernetică a sistemelor informaţionale de stat, precum şi exercită şi alte atribuţii în conformitate cu statutul acesteia aprobat de către Guvern.

(3) Instituţia publică Serviciul Tehnologia Informaţiei şi Securitate Cibernetică, în limita competenţelor, administrează infrastructura tehnologiilor informaţionale ale autorităţilor şi instituţiilor publice, exercită atribuţiile administratorului tehnic şi asigură mentenanţa sistemelor informaţionale de stat, asigură securitatea cibernetică a acestora, precum şi exercită şi alte atribuţii în conformitate cu statutul acesteia aprobat de către Guvern.

(4) Instituţia publică Agenţia Servicii Publice exercită, în numele Guvernului, atribuţiile de posesor al resurselor informaţionale de bază.

(5) Alte autorităţi şi instituţii publice formează şi utilizează resurse informaţionale departamentale şi teritoriale în scopul exercitării atribuţiilor acestora şi participă la formarea resurselor informaţionale de bază în limita competenţelor stabilite de către Guvern.

[Art.23 în redacţia LP135 din 16.07.20, MO199-204/07.08.20 art.410; în

vigoare 07.08.20]

[Art.24 abrogat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

[Art.25 abrogat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 26. Sursele de finanţare a activităţii de formare şi utilizare a resurselor informaţionale de stat

(1) Sursele de finanţare a activităţii de formare şi utilizare a resurselor informaţionale de stat sînt alocaţiile bugetare pentru întreţinerea instituţiilor publice, aprobate prin legea bugetului pe anul respectiv, precum şi mijloacele autorităților publice, ale instituțiilor publice și ale entităților implicate în astfel de activități, mijloace obţinute din prestarea contra plată a serviciilor aferente resurselor informaţionale de stat.

[Art.26 al.(1) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(2) La formarea şi utilizarea resurselor informaționale pot fi atrase mijloacele financiare provenite din proiecte de asistență externă.

[Art.26 al.(2) în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Capitolul VI
UTILIZAREA RESURSELOR INFORMAȚIONALE

Articolul 27. Accesul la resursele informaţionale de stat

Resursele informaţionale de stat sînt publice şi accesibile tuturor. Excepţie face informaţia documentată atribuită, conform legii, categoriei de informaţie cu acces limitat.

Articolul 28. Realizarea dreptului de acces la informaţia din resursele informaţionale de stat

(1) Utilizatorii beneficiază de drepturi egale de acces la resursele informaţionale de stat şi nu sînt obligaţi să justifice, în faţa posesorilor acestor resurse, necesitatea obţinerii informaţiei solicitate, excepţie fiind informaţia cu acces limitat.

(2) Posesorii de resurse informaționale asigură utilizatorii cu informație din resursele informaționale de stat, în conformitate cu legislația în vigoare, prin intermediul platformei de interoperabilitate.

Articolul 29. Dreptul la obţinerea informaţiei documentate din resursele informaţionale de stat

(1) Autoritățile şi instituțiile publice, persoanele fizice şi persoanele juridice au dreptul să obțină informații documentate.

[Art.29 al.(1) în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(2) Dreptul la obţinerea informaţiei documentate poate fi limitat în condiţiile legii.

(3) Realizarea dreptului de a obţine informaţie documentată nu trebuie să lezeze drepturile şi interesele legitime ale altor persoane.

(4) Organele de urmărire penală au dreptul, în limitele competenţei şi în conformitate cu legislaţia în vigoare, la informaţie documentată cu acces limitat.

(5) Subiecții care sunt obligați să prezinte autorităților şi instituțiilor publice informații documentate nu-şi pierd drepturile asupra documentelor prezentate şi nici asupra utilizării informaţiei pe care acestea o conțin.

[Art.29 al.(5) în redacția LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

Articolul 30. Accesul persoanei fizice şi al persoanei juridice la informaţia documentată despre sine

(1) Persoana fizică sau persoana juridică ale cărei resurse informaţionale conțin informaţii documentate despre alte persoane este obligată să le acorde accesul la informațiile respective.

[Art.30 al.(1) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(2) Persoanele fizice şi persoanele juridice au dreptul:

de acces la informaţia documentată despre sine;

de a preciza informaţia documentată despre sine pentru asigurarea plenitudinii şi exactităţii ei;

de a contesta informaţia documentată despre sine în modul stabilit de legislaţie;

de a cunoaşte cine şi în ce scop acumulează sau utilizează informaţia documentată despre sine.

(3) Refuzul de a permite accesul persoanei la informaţia documentată despre sine şi tăinuirea acestei informaţii pot fi atacate în justiţie.

Articolul 31. Modul de furnizare a informaţiilor

(1) Modul de furnizare a informațiilor se stabilește în conformitate cu legislația în vigoare cu privire la schimbul de date și interoperabilitate.

(2) Autoritățile publice, instituțiile publice şi entitățile responsabile de formarea şi utilizarea resurselor informaţionale de stat asigură condiţii pentru furnizarea unei informaţii documentate complete în conformitate cu obligaţiile ce le revin, conform regulamentelor lor şi altor acte normative.

[Art.31 al.(2) modificat prin LP135 din 16.07.20, MO199-204/07.08.20 art.410; în vigoare 07.08.20]

(3) Modul de colectare şi de prelucrare a informaţiilor documentate cu acces limitat, regulile de protecţie a acestora şi de acces la ele se stabilesc de Guvern.

(4) Raporturile dintre proprietarii, posesorii de resurse informaţionale şi utilizatorii de informație din aceste resurse se reglementează în conformitate cu legislația în vigoare privind schimbul de date şi interoperabilitate.

Capitolul VII

RĂSPUNDEREA

Articolul 32. Răspunderea pentru încălcarea prezentei legi

Încălcarea prezentei legi se pedepseşte pe cale civilă, administrativă sau penală, în condiţiile legii.

PARLAMENTUL

LEGE Nr. 245 din 27-11-2008

cu privire la secretul de stat

Publicat : 27-02-2009 în Monitorul Oficial Nr. 45-46 art. 123

MODIFICAT LP265 din 23.11.18, MO1-5/04.01.19 art.8; în vigoare 04.01.19

Capitolul I
DISPOZIŢII GENERALE

Articolul 1. Noţiuni

În sensul prezentei legi se definesc următoarele noţiuni:

certificat de securitate – document ce atestă dreptul persoanei juridice, cu excepţia autorităţii publice, de a desfăşura activităţi ce ţin de utilizarea informaţiilor atribuite la secret de stat, de crearea mijloacelor de protejare a informaţiei, de realizarea măsurilor şi/sau prestarea serviciilor de protecţie a secretului de stat;

dreptul de acces la secretul de stat – dreptul persoanei fizice de acces la secretul de stat, iar al persoanei juridice – de a efectua lucrări cu utilizarea informaţiilor atribuite la secret de stat, perfectat în modul stabilit;

grad de secretizare – categorie ce caracterizează importanţa informaţiilor atribuite la secret de stat, gradul de limitare a accesului la ele şi gradul de protecţie a lor de către stat;

mijloace de protejare a informaţiilor – mijloace tehnice, criptografice, de program şi de altă natură menite să protejeze informaţiile atribuite la secret de stat, mijloacele prin care acestea sînt realizate, precum şi mijloacele de verificare a eficienţei protejării informaţiilor;

parafă de secretizare – menţiune aplicată pe purtătorul material de informaţii atribuite la secret de stat şi/sau indicată în documentaţia de însoţire a acestuia, care atestă gradul de secretizare a informaţiilor conţinute de purtător;

pierderea informaţiilor atribuite la secret de stat – ieşirea, inclusiv temporară, din posesia sau folosirea legală a informaţiilor atribuite la secret de stat drept rezultat al pierderii, sustragerii sau distrugerii neautorizate a acestora;

protecţia secretului de stat – complex de măsuri organizatorico-juridice, tehnico-inginereşti, criptografice, operative de investigaţii şi de altă natură, destinate prevenirii divulgării sau pierderii informaţiilor atribuite la secret de stat;

purtători materiali de informaţii atribuite la secret de stat – obiecte materiale, inclusiv cîmpuri fizice, în care informaţiile atribuite la secret de stat sînt expuse în formă de texte, semne, simboluri, imagini, semnale, soluţii tehnice, procese etc.;

secret de stat – informaţii protejate de stat în domeniul apărării naţionale, economiei, ştiinţei şi tehnicii, relaţiilor externe, securităţii statului, asigurării ordinii de drept şi activităţii autorităţilor publice, a căror divulgare neautorizată sau pierdere este de natură să aducă atingere intereselor şi/sau securităţii Republicii Moldova.

Articolul 2. Scopul şi sfera de aplicare a legii

(1) Prezenta lege stabileşte cadrul juridic de protecţie a secretului de stat în scopul asigurării intereselor şi/sau securităţii Republicii Moldova. Protejarea secretului de stat se realizează prin organizarea sistemului naţional de protecţie a secretului de stat.

(2) Prevederile prezentei legi sînt executorii şi pentru cetăţenii străini şi apatrizii care şi-au asumat obligaţia sau sînt obligaţi, conform statutului lor, să execute prevederile legislaţiei Republicii Moldova cu privire la secretul de stat.

(3) Informaţiile transmise Republicii Moldova, ce constituie secret al unui stat străin sau al unei organizaţii internaţionale, sînt protejate în modul stabilit de prezenta lege. În cazul în care tratatul internaţional la care Republica Moldova este parte conţine alte prevederi referitoare la protecţia secretului unui stat străin sau al unei organizaţii internaţionale, se aplică prevederile tratatului internaţional.

Articolul 3. Legislaţia cu privire la secretul de stat

Legislaţia cu privire la secretul de stat are la bază Constituţia Republicii Moldova, prezenta lege, alte acte normative ce reglementează protecţia secretului de stat, precum şi tratatele internaţionale la care Republica Moldova este parte.

Articolul 4. Sistemul naţional de protecţie a
secretului de stat

(1) Sistemul naţional de protecţie a secretului de stat include totalitatea organelor de protecţie a secretului de stat, a metodelor şi mijloacelor de protejare a informaţiilor şi a purtătorilor materiali de informaţii atribuite la secret de stat, precum şi totalitatea măsurilor întreprinse în acest domeniu.

(2) Sistemul naţional de protecţie a secretului de stat vizează:

a) protecţia juridică – ansamblul prevederilor conţinute în actele legislative şi normative ce reglementează protecţia secretului de stat;

b) protecţia prin măsuri procedurale – ansamblul reglementărilor prin care deţinătorii de informaţii atribuite la secret de stat stabilesc măsuri interne de lucru şi de ordine interioară în vederea realizării protecţiei informaţiilor;

c) protecţia fizică – ansamblul activităţilor de pază, de asigurare a securităţii şi de apărare a informaţiilor atribuite la secret de stat prin măsuri şi mijloace de control fizic;

d) protecţia sistemelor informaţionale şi de telecomunicaţii – ansamblul activităţilor de asigurare a securităţii informaţiilor atribuite la secret de stat prin aplicarea metodelor şi mijloacelor criptografice şi tehnice de protecţie a informaţiilor, precum şi a procedurilor tehnico-organizatorice;

e) protecţia personalului – ansamblul verificărilor şi al măsurilor ce vizează cetăţenii cărora li se perfectează dreptul de acces la secretul de stat sau care au acces la acesta în scopul prevenirii şi înlăturării riscurilor pentru securitatea şi protecţia secretului de stat.

(3) Sistemul naţional de protecţie a secretului de stat este destinat:

a) să prevină accesul neautorizat, divulgarea şi pierderea secretului de stat;

b) să identifice împrejurările, precum şi persoanele care, prin acţiunile sau inacţiunile lor, pot pune în pericol securitatea secretului de stat;

c) să garanteze că informaţiile atribuite la secret de stat sînt accesibile exclusiv persoanelor îndreptăţite să le cunoască în legătură cu îndeplinirea atribuţiilor de serviciu sau în baza unui alt temei legal;

d) să asigure securitatea sistemelor de telecomunicaţii, a sistemelor informaţionale şi a reţelelor de transmitere a secretului de stat.

Articolul 5. Atribuţiile autorităţilor publice în domeniul

protecţiei secretului de stat

(1) Parlamentul:

a) reglementează din punct de vedere legislativ relaţiile în domeniul secretului de stat;

b) stabileşte atribuţiile persoanelor cu funcţii de răspundere din cadrul Secretariatului Parlamentului privind asigurarea protecţiei secretului de stat în Parlament;

c) exercită controlul parlamentar asupra executării legislaţiei privind secretul de stat.

(2) Preşedintele Republicii Moldova:

a) încheie tratate internaţionale privind utilizarea în comun şi protecţia informaţiilor atribuite la secret de stat;

b) stabileşte atribuţiile persoanelor responsabile de asigurarea protecţiei secretului de stat în cadrul Aparatului Preşedintelui Republicii Moldova;

c) în limita competenţelor sale, exercită alte atribuţii ce ţin de soluţionarea problemelor care apar în legătură cu secretizarea, desecretizarea şi protecţia informaţiei.

(3) Guvernul:

a) organizează executarea prezentei legi;

b) aprobă structura, componenţa şi regulamentul Comisiei interdepartamentale pentru protecţia secretului de stat;

c) aprobă Nomenclatorul persoanelor cu funcţii de răspundere cu împuterniciri de atribuire a informaţiilor la secret de stat, precum şi Nomenclatorul informaţiilor atribuite la secret de stat;

d) încheie acorduri interguvernamentale privind protecţia reciprocă a informaţiilor atribuite la secret de stat;

e) aprobă Regulamentul cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice;

f) aprobă Regulamentul cu privire la obiectivele cu regim special, lista obiectivelor cu regim special, lista obiectivelor a căror vizitare este temporar interzisă cetăţenilor străini;

g) stabileşte tipurile de compensaţii, mărimea şi modul de acordare a acestora cetăţenilor care efectuează lucrări legate de accesul la secretul de stat;

h) stabileşte modul de determinare a mărimii prejudiciului cauzat sau care poate fi cauzat intereselor şi/sau securităţii Republicii Moldova ori intereselor autorităţilor publice prin divulgarea sau pierderea informaţiilor atribuite la secret de stat, precum şi a prejudiciului cauzat proprietarului informaţiilor în urma secretizării lor;

i) adoptă decizii privind transmiterea informaţiilor atribuite la secret de stat unor state străine sau organizaţii internaţionale;

j) poate modifica, prin hotărîre, modul de acces la secretul de stat în cazul declarării stării de urgenţă, de asediu sau de război;

k) în limita competenţelor, exercită şi alte atribuţii în domeniul secretului de stat.

(4) Autorităţile publice centrale şi locale, în colaborare cu Serviciul de Informaţii şi Securitate:

a) asigură protecţia informaţiilor atribuite la secret de stat elaborate de ele, precum şi a informaţiilor atribuite la secret de stat ce le sînt transmise de către alte autorităţi publice sau persoane juridice;

b) asigură protecţia informaţiilor atribuite la secret de stat în unităţile din subordine, conform prevederilor legislaţiei;

c) aprobă nomenclatoarele departamentale de informaţii ce urmează a fi secretizate şi nomenclatoarele funcţiilor colaboratorilor cărora urmează să li se perfecteze dreptul de acces la secretul de stat;

d) organizează funcţionarea subdiviziunilor interioare de protecţie a secretului de stat;

e) asigură, în limita competenţei lor, realizarea măsurilor de control în privinţa cetăţenilor cărora urmează să li se perfecteze dreptul de acces la secretul de stat şi solicită Serviciului de Informaţii şi Securitate realizarea măsurilor de control ce ţin de competenţa acestuia;

f) prezintă organelor competente propuneri privind perfecţionarea sistemului naţional de protecţie a secretului de stat;

g) în limita competenţei, exercită şi alte atribuţii în domeniul secretului de stat.

(5) Serviciul de Informaţii şi Securitate:

a) elaborează, împreună cu autorităţile administraţiei publice şi Comisia interdepartamentală pentru protecţia secretului de stat, şi prezintă Guvernului spre aprobare proiecte de acte normative în domeniul protecţiei secretului de stat;

b) acordă asistenţă de specialitate autorităţilor publice şi altor persoane juridice în organizarea protecţiei secretului de stat;

c) participă la elaborarea şi realizarea măsurilor de protecţie a secretului de stat în cadrul autorităţilor publice şi al altor persoane juridice;

d) efectuează controlul asupra asigurării protecţiei secretului de stat în cadrul autorităţilor publice (controlul interdepartamental) şi în cadrul altor persoane juridice;

e) la cererea conducătorilor autorităţilor publice şi ai altor persoane juridice, întreprinde măsuri de control în privinţa cetăţenilor cărora urmează să li se perfecteze dreptul de acces la secretul de stat;

f) participă, în modul stabilit, la eliberarea certificatelor de securitate pentru persoanele juridice în vederea efectuării lucrărilor cu utilizarea informaţiilor atribuite la secret de stat şi la controlul asupra respectării de către titularii certificatelor de securitate a condiţiilor care au constituit temei pentru acordarea acestora;

g) efectuează controlul şi expertiza obiectivelor cu regim special în partea ce ţine de respectarea cerinţelor privind protecţia secretului de stat;

h) organizează şi coordonează certificarea şi expertiza mijloacelor de protejare criptografică şi tehnică a secretului de stat;

i) creează sisteme guvernamentale de telecomunicaţii, asigură funcţionarea, securitatea, întreţinerea, dezvoltarea şi modernizarea acestor sisteme în scopul asigurării unui schimb protejat de informaţii atribuite la secret de stat;

j) conlucrează cu Comisia interdepartamentală pentru protecţia secretului de stat în chestiuni ce ţin de aplicarea prezentei legi;

k) constată cazurile de încălcare a normelor privind protecţia secretului de stat;

k[1]) asigură curieratul diplomatic şi exercită controlul asupra circuitului informaţiilor atribuite la secret de stat şi al informaţiilor de serviciu între Ministerul Afacerilor Externe şi Integrării Europene şi misiunile diplomatice şi oficiile consulare ale Republicii Moldova din străinătate;

l) în limita competenţelor, exercită şi alte atribuţii în domeniul secretului de stat.

(6) Comisia interdepartamentală pentru protecţia secretului de stat:

a) elaborează principiile conceptuale ale politicii de stat în domeniul protecţiei secretului de stat;

b) creează şi perfecţionează sistemul de protecţie a secretului de stat, baza lui organizatorico-juridică;

c) asigură dirijarea metodico-organizatorică a sistemului de protecţie a secretului de stat, funcţionarea lui;

d) exercită controlul tehnic privind aplicarea legislaţiei cu privire la protecţia secretului de stat în cadrul organelor administraţiei publice, la întreprinderi, instituţii, organizaţii şi subdiviziunile lor structurale, indiferent de forma de proprietate, la reprezentanţele diplomatice şi alte instituţii ale Republicii Moldova din străinătate;

e) organizează şi coordonează activitatea organelor administraţiei publice, întreprinderilor, instituţiilor, organizaţiilor şi subdiviziunilor structurale ale acestora, indiferent de forma de proprietate, privind asigurarea regimului secret şi a protecţiei tehnice a informaţiilor despre comenzile de stat, contractele şi programele referitoare la apărarea naţională, lucrările de mobilizare, securitate, mărimea rezervelor de stat, precum şi la realizarea unor decizii din domeniul politicii externe;

f) elaborează, împreună cu autorităţile administraţiei publice şi cu Serviciul de Informaţii şi Securitate, şi prezintă Guvernului spre aprobare proiecte de acte

normative în domeniul protecţiei secretului de stat;

g) organizează investigaţii ştiinţifice cu privire la elaborarea bazelor conceptuale ale politicii de stat în domeniul protecţiei secretului de stat, a criteriilor de evaluare a prejudiciului adus statului în cazul scurgerii informaţiei care constituie secret de stat;

h) efectuează, împreună cu organele administraţiei publice şi organizaţiile ştiinţifice, o analiză a dezvoltării mijloacelor tehnice în domeniul protecţiei informaţiei;

i) înregistrează, în conformitate cu prezenta lege, nomenclatoarele departamentale de informaţii care urmează a fi secretizate;

j) elaborează Nomenclatorul informaţiilor atribuite la secret de stat şi îl prezintă Guvernului spre aprobare, face propuneri privind modificarea şi completarea acestui nomenclator;

k) eliberează certificate de securitate în modul stabilit de prezenta lege;

l) controlează termenele de acţiune a parafei de secretizare stabilite anterior pentru informaţiile păzite, informează Guvernul despre necesitatea prelungirii termenelor de secretizare a informaţiilor ce prezintă o valoare deosebită pentru stat;

m) elaborează şi prezintă Guvernului propuneri de pronosticare a cheltuielilor bugetului de stat pentru măsurile de protecţie a secretului de stat;

n) colaborează, în limita competenţelor, cu organele similare ale altor state în domeniul protecţiei reciproce a informaţiei secrete transmise în baza contractelor (acordurilor) internaţionale, soluţionează chestiunile protecţiei organizatorico-juridice a informaţiilor, participă la expertiza proiectelor contractelor (acordurilor) menţionate.

Capitolul II

Atribuirea informaţiilor la secret de stat

Articolul 6. Principiile de atribuire a informaţiilor la secret de stat şi de secretizare a acestor informaţii

(1) Atribuirea informaţiilor la secret de stat şi secretizarea acestora se efectuează în baza principiilor legalităţii, argumentării şi oportunităţii.

(2) Legalitatea atribuirii informaţiilor la secret de stat şi a secretizării acestora constă în corespunderea acestor informaţii cu prevederile art.7 şi 8 din prezenta lege şi cu legislaţia privind secretul de stat.

(3) Argumentarea atribuirii informaţiilor la secret de stat şi a secretizării acestora constă în stabilirea caracterului raţional al secretizării unor informaţii concrete, a eventualelor consecinţe economice şi de altă natură ale acestei acţiuni, ţinînd cont de echilibrul dintre interesele primordiale ale statului, ale societăţii şi ale cetăţeanului.

(4) Oportunitatea atribuirii informaţiilor la secret de stat şi a secretizării acestora constă în stabilirea unor restricţii privind accesul şi răspîndirea informaţiilor respective fie din momentul elaborării/primirii lor, fie din timp.

Articolul 7. Informaţiile atribuite la secret de stat

(1) În modul stabilit de prezenta lege sînt atribuite la secret de stat informaţiile:

1) din domeniul apărării naţionale privind:

a) conţinutul planurilor strategice şi operative, al documentelor ce ţin de conducerea operaţiunilor de luptă privind pregătirea şi derularea operaţiunilor, desfăşurarea strategică, operativă şi de mobilizare a trupelor, alţi indicatori importanţi ce caracterizează organizarea, efectivul, dislocarea, pregătirea de luptă şi de mobilizare, armamentul şi asigurarea tehnico-materială a Forţelor Armate ale Republicii Moldova;

b) direcţiile de dezvoltare a unor tipuri de armament, de tehnică militară şi specială, cantitatea şi caracteristicile lor tehnico-tactice, organizarea şi tehnologiile de producere, lucrările ştiinţifice teoretice şi experimentale legate de crearea modelelor noi de armament, tehnică militară şi specială sau modernizarea acestora, alte lucrări planificate sau efectuate în interesele apărării naţionale;

c) forţele şi mijloacele protecţiei civile, capacităţile de care dispun localităţile şi unele obiective separate pentru protecţia, evacuarea şi dispersarea populaţiei, asigurarea activităţilor sociale vitale ale populaţiei şi a activităţii de producere a persoanelor juridice în perioada de război, de asediu sau de urgenţă, precum şi în cazul situaţiilor excepţionale;

d) dislocarea, destinaţia, gradul de pregătire şi de securitate a obiectivelor cu regim special, proiectarea, construirea şi exploatarea acestora, repartizarea terenului, subsolului şi acvatoriului pentru asemenea obiective;

e) datele şi caracteristicile geodezice, gravimetrice, cartografice şi hidrometeorologice care prezintă importanţă pentru apărarea statului;

2) din domeniul economiei, ştiinţei şi tehnicii privind:

a) planurile şi potenţialul de mobilizare a economiei naţionale, rezervele şi volumul livrărilor de materiale strategice, datele generalizate despre nomenclatura şi nivelul stocurilor, volumul livrărilor, alocării, depunerii, împrospătării acestora, amplasarea şi volumul real al rezervelor materiale de stat;

b) utilizarea transporturilor, comunicaţiilor, a potenţialului altor ramuri şi obiective ale infrastructurii naţionale în scopul asigurării capacităţii de apărare şi a securităţii statului;

c) planurile, conţinutul, volumul, finanţarea şi îndeplinirea comenzilor de stat pentru asigurarea securităţii statului şi a necesităţilor sale de apărare;

d) planurile, volumul şi alte caracteristici importante privind extragerea, producerea şi realizarea unor tipuri strategice de materie primă şi produse;

e) operaţiunile ce ţin de confecţionarea semnelor băneşti şi a titlurilor de valoare emise de stat, păstrarea şi protecţia lor contra falsificării, emiterea, schimbul şi retragerea lor din circulaţie;

f) lucrările ştiinţifice teoretice, experimentale de construcţii şi proiectare, în baza cărora pot fi create tehnologii avansate, tipuri noi de producţie, produse şi procese tehnologice, care prezintă importanţă pentru apărarea şi economia naţională sau care influenţează esenţial activitatea economică externă, interesele şi/sau securitatea statului;

3) din domeniul relaţiilor externe privind:

a) activitatea de politică externă, relaţiile economice externe ale Republicii Moldova, a căror divulgare prematură poate cauza prejudicii intereselor şi/sau securităţii statului;

b) colaborarea militară, tehnico-ştiinţifică şi de altă natură a Republicii Moldova cu statele străine şi organizaţiile internaţionale, dacă divulgarea acestor informaţii va cauza, inevitabil, prejudicii intereselor şi/sau securităţii statului;

c) activitatea externă a statului în domeniile financiar, creditar şi valutar, dacă divulgarea acestor informaţii va cauza prejudicii intereselor şi/sau securităţii statului;

4) din domeniul securităţii statului şi asigurării ordinii de drept privind:

a) efectivul, forţele, conţinutul, planurile, organizarea, finanţarea şi asigurarea tehnico-materială, formele, tactica, metodele, mijloacele şi rezultatele activităţilor de informaţii, de contrainformaţii şi operative de investigaţii;

a[1]) efectivul, forţele, conţinutul, planurile, organizarea, finanţarea şi asigurarea tehnico-materială, formele, tactica, metodele, mijloacele activităților de desfăşurare a testării integrităţii profesionale, cu excepţia datelor din raportul privind rezultatele evaluării integrităţii instituţionale;

b) persoanele care colaborează sau au colaborat confidenţial cu organele care desfăşoară activităţi de informaţii, de contrainformaţii şi operative de investigaţii;

c) forţele, mijloacele şi metodele de asigurare a protecţiei de stat părţii vătămate, martorilor şi altor persoane care acordă ajutor în procesul penal;

d) paza frontierei de stat a Republicii Moldova;

e) planurile, organizarea, finanţarea, efectivul, forţele, mijloacele şi metodele de asigurare a securităţii persoanelor beneficiare de protecţie de stat, precum şi paza sediilor de lucru şi a reşedinţelor acestora;

f) sistemele de telecomunicaţii guvernamentale şi alte tipuri de reţele de telecomunicaţii electronice care asigură necesităţile autorităţilor publice, apărării naţionale, securităţii statului şi menţinerii ordinii publice;

g) organizarea, conţinutul, starea şi planurile de dezvoltare a protecţiei criptografice şi tehnice a secretului de stat, conţinutul şi rezultatele cercetărilor ştiinţifice în domeniul criptografiei referitor la protecţia secretului de stat;

h) sistemele şi mijloacele de protecţie criptografică a secretului de stat, proiectarea, producerea, tehnologiile de producere şi utilizarea acestora;

i) cifrurile de stat, elaborarea, crearea, tehnologiile de producere şi utilizarea acestora;

j) organizarea regimului secret în cadrul autorităţilor publice şi în al altor persoane juridice, planurile şi măsurile în domeniul protecţiei secretului de stat;

k) alte metode, forme şi mijloace de protecţie a secretului de stat;

5) din sfera activităţii autorităţilor publice privind:

a) conţinutul extraselor, comentariilor, proiectelor, părţilor acestora, al altor acte de uz intern ale autorităţilor publice, a căror divulgare ar putea conduce la divulgarea informaţiilor atribuite la secret de stat;

b) activitatea de elaborare, modificare, completare, definitivare a actelor oficiale, alte proceduri şi activităţi ale autorităţilor publice de colectare şi prelucrare a informaţiilor care, în modul prevăzut de legislaţie, urmează să fie atribuite la secret de stat;

c) activitatea de examinare şi deliberare în cadrul autorităţilor publice şi între acestea în probleme din domeniile în care informaţiile sînt atribuite la secret de stat.

(2) Motivarea necesităţii de a atribui informaţiile la secret de stat, în baza principiilor de atribuire a informaţiilor la secret de stat şi secretizare a acestora, revine autorităţilor publice şi altor persoane juridice care au elaborat/primit aceste informaţii.

Articolul 8. Informaţiile care nu se atribuie la secret de stat

(1) Nu se atribuie la secret de stat şi nu pot fi secretizate informaţiile privind:

a) faptele de încălcare a drepturilor şi libertăţilor omului şi ale cetăţeanului;

b) starea mediului înconjurător, calitatea produselor alimentare şi a obiectelor de uz casnic;

c) accidentele, catastrofele, fenomenele naturale periculoase şi alte evenimente extraordinare care periclitează securitatea cetăţenilor;

d) starea sănătăţii populaţiei, nivelul ei de trai, inclusiv alimentaţia, îmbrăcămintea, deservirea medicală şi asigurarea socială, indicatorii sociodemografici;

e) starea sănătăţii persoanelor care ocupă funcţii de demnitate publică;

f) faptele de încălcare a legii de către autorităţile publice şi persoanele cu funcţii de răspundere din cadrul acestora;

g) starea reală de lucruri în domeniul învăţămîntului, culturii, comerţului, agriculturii şi al ordinii de drept.

Nu se atribuie la secret de stat şi nu pot fi secretizate şi alte informaţii conform legislaţiei naţionale şi tratatelor internaţionale la care Republica Moldova este parte.

(2) Se interzice secretizarea informaţiilor în cazul în care aceasta ar putea limita accesul la informaţiile de interes public, s-ar putea răsfrînge negativ asupra realizării programelor de stat şi de ramură ale dezvoltării social-economice şi culturale sau ar putea reţine concurenţa dintre agenţii economici.

Articolul 9. Nomenclatorul informaţiilor atribuite

la secret de stat

(1) În scopul promovării unei politici de stat unice în domeniul atribuirii informaţiilor la secret de stat şi al secretizării lor, Guvernul aprobă Nomenclatorul informaţiilor atribuite la secret de stat în care sînt incluse şi autorităţile publice cu împuterniciri de dispoziţie asupra acestor informaţii.

(2) Nomenclatorul informaţiilor atribuite la secret de stat se publică în Monitorul Oficial al Republicii Moldova şi poate fi revizuit în caz de necesitate.

Articolul 10. Nomenclatoare departamentale de

informaţii care urmează a fi secretizate

(1) În baza şi în limitele Nomenclatorului informaţiilor atribuite la secret de stat şi în scopul concretizării şi sistematizării informaţiilor în domeniile lor de activitate, autorităţile publice indicate în Nomenclator elaborează nomenclatoare departamentale detaliate de informaţii care urmează a fi secretizate. În caz de necesitate, pot fi elaborate nomenclatoare interdepartamentale detaliate de informaţii care urmează a fi secretizate.

(2) Persoanele juridice care efectuează lucrări cu utilizarea informaţiilor atribuite la secret de stat elaborează, după caz, în coordonare cu beneficiarul acestor lucrări, nomenclatoare detaliate separate de informaţii care urmează a fi secretizate.

(3) Nomenclatoarele departamentale de informaţii care urmează a fi secretizate conţin informaţii asupra cărora au împuterniciri de dispoziţie autorităţile publice în cauză, în acestea stabilindu-se gradele şi termenele de secretizare a informaţiilor. Nomenclatoarele menţionate trebuie să corespundă Nomenclatorului informaţiilor atribuite la secret de stat.

(4) Nomenclatoarele departamentale de informaţii care urmează a fi secretizate, precum şi modificările şi completările la acestea, coordonate cu Comisia interdepartamentală pentru protecţia secretului de stat, se aprobă de către conducătorii autorităţilor publice cu împuterniciri de dispoziţie asupra informaţiilor în cauză şi nu sînt date publicităţii. Cîte un exemplar al nomenclatoarelor departamentale de informaţii care urmează a fi secretizate se transmite pentru înregistrare Comisiei interdepartamentale pentru protecţia secretului de stat şi Serviciului de Informaţii şi Securitate.

(5) Conducătorii autorităţilor publice cu împuterniciri de dispoziţie asupra informaţiilor atribuite la secret de stat sînt obligaţi să revizuiască periodic, cel puţin o dată la 5 ani, conţinutul nomenclatoarelor departamentale de informaţii care urmează a fi secretizate în ceea ce priveşte argumentarea secretizării informaţiilor şi corespunderea cu gradele de secretizare stabilite anterior.

Capitolul III

Secretizarea şi desecretizarea informaţiilor

Articolul 11. Gradele de secretizare a informaţiilor atribuite la secret de stat şi parafele de secretizare pentru purtătorii materiali de asemenea informaţii

(1) Gradul de secretizare a informaţiilor atribuite la secret de stat trebuie să corespundă gravităţii prejudiciilor ce pot fi cauzate intereselor şi/sau securităţii Republicii Moldova în cazul divulgării sau pierderii acestor informaţii.

(2) Sînt stabilite 4 grade de secretizare a informaţiilor atribuite la secret de stat şi 4 parafe de secretizare corespunzătoare pentru purtătorii materiali de asemenea informaţii:

a) „Strict secret” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate aduce prejudicii deosebit de grave intereselor şi/sau securităţii Republicii Moldova;

b) „Secret” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate dăuna grav intereselor şi/sau securităţii Republicii Moldova;

c) „Confidenţial” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate dăuna intereselor şi/sau securităţii Republicii Moldova;

d) „Restricţionat” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate fi în dezavantajul intereselor şi/sau securităţii Republicii Moldova sau poate să conducă la divulgarea unei informaţii secretizate cu parafa „Strict secret”, „Secret” sau „Confidenţial”.

(3) Nu se admite aplicarea parafelor de secretizare menţionate la alin.(2) în vederea secretizării informaţiilor care nu sînt atribuite la secret de stat.

(4) Pagini, paragrafe, secţiuni dintr-un anumit document sau din anexele la acesta pot necesita atribuirea unor grade diferite de secretizare şi trebuie, în acest caz, să poarte menţiunea corespunzătoare. Gradul de secretizare atribuit documentului ca întreg coincide cu acela al părţii sale căreia i s-a atribuit gradul de secretizare cel mai înalt.

(5) Purtătorii materiali de informaţii atribuite la secret de stat destinate unor anumite persoane sînt marcaţi suplimentar cu menţiunea „Personal”, iar cei ce se referă la mobilizare – cu litera „M”.

Articolul 12. Modul de secretizare a informaţiilor

(1) Drept temei pentru secretizarea informaţiilor elaborate/primite în cadrul activităţii de administrare, de producţie, ştiinţifice şi de altă natură a autorităţilor publice şi a altor persoane juridice este corespunderea lor cu art.7 şi 8 din prezenta lege, cu Nomenclatorul informaţiilor atribuite la secret de stat şi cu nomenclatoarele departamentale de informaţii care urmează a fi secretizate. La secretizarea acestor informaţii, pe purtătorii lor materiali se aplică parafa de secretizare corespunzătoare.

(2) În cazul în care informaţiile elaborate/primite nu pot fi identificate cu informaţiile ce se conţin în nomenclatorul corespunzător, persoanele cu funcţii de răspundere din cadrul autorităţilor publice şi al altor persoane juridice sînt obligate să asigure secretizarea preliminară a informaţiilor elaborate/primite conform gradului de secretizare estimat şi, în termen de o lună, să prezinte persoanei cu funcţie de răspundere care a aprobat nomenclatorul menţionat propuneri privind modificarea/completarea lui.

(3) Conducătorii autorităţilor publice şi ai altor persoane juridice care au aprobat nomenclatorul respectiv sînt obligaţi, în termen de 3 luni, să organizeze evaluarea de către experţi a propunerilor primite şi să ia decizia de modificare/completare a nomenclatorului în vigoare sau de eliminare a parafei de secretizare atribuite preliminar. În caz de necesitate şi în modul stabilit, se înaintează propuneri argumentate privind modificarea şi/sau completarea Nomenclatorului informaţiilor atribuite la secret de stat.

(4) Nomenclatoarele funcţiilor angajaţilor cărora urmează să li se perfecteze dreptul de acces la secretul de stat se întocmesc cu consultarea Serviciului de Informaţii şi Securitate şi se aprobă de către conducătorii autorităţilor publice şi ai altor persoane juridice care elaborează/primesc asemenea informaţii.

Articolul 13. Termenele de secretizare a informaţiilor

(1) Pentru informaţiile avînd gradul de secretizare „Strict secret” se stabileşte un termen de secretizare de pînă la 25 de ani, pentru informaţiile cu gradul „Secret” – un termen de pînă la 15 ani, pentru informaţiile cu gradul „Confidenţial” – de pînă la 10 ani şi pentru informaţiile cu gradul „Restricţionat” – de pînă la 5 ani.

(2) Pentru informaţiile despre persoanele care colaborează sau au colaborat confidenţial cu organe ce desfăşoară activităţi de informaţii, de contrainformaţii şi operative de investigaţii se stabileşte un termen de secretizare nelimitat.

(3) În cazuri excepţionale, pentru anumite informaţii atribuite la secret de stat, Comisia interdepartamentală pentru protecţia secretului de stat poate prelungi termenul de secretizare.

(4) Termenul de secretizare a informaţiilor începe din ziua în care pe purtătorul material de informaţii atribuite la secret de stat a fost aplicată parafa de secretizare.

Articolul 14. Menţiunile aplicate pe purtătorii materiali

de informaţii atribuite la secret de stat

(1) Purtătorii materiali de informaţii atribuite la secret de stat trebuie să conţină:

a) parafa de secretizare;

b) numărul de înregistrare;

c) data şi termenul de secretizare a informaţiilor;

d) funcţia, numele, prenumele şi semnătura persoanei cu funcţie de răspundere care a secretizat informaţiile.

(2) Parafa de secretizare trebuie să fie aplicată în partea superioară a fiecărei pagini, iar fiecare pagină va fi numerotată. Dacă documentul urmează să fie distribuit în mai multe exemplare, fiecare dintre acestea va purta un număr de exemplare, care apare pe prima pagină împreună cu numărul total de pagini.

(3) În cazul în care menţiunile nu pot fi aplicate nemijlocit pe purtătorul material de informaţii atribuite la secret de stat, ele se indică în documentaţia de însoţire a acestuia.

Articolul 15. Modificarea parafei de secretizare

a purtătorilor materiali de informaţii

atribuite la secret de stat

(1) Modificarea parafei de secretizare a purtătorilor materiali de informaţii atribuite la secret de stat se face în cazurile în care se modifică gradul de secre-

tizare al informaţiilor conţinute de aceştia.

(2) Modificarea parafei de secretizare în legătură cu reducerea gradului de secretizare al categoriilor de informaţii prevăzute în Nomenclatorul informaţiilor atribuite la secret de stat şi în nomenclatoarele departamentale de informaţii care urmează a fi secretizate se efectuează în termen de 6 luni. În toate celelalte cazuri, modificarea parafei de secretizare a purtătorilor materiali de informaţii atribuite la secret de stat se efectuează în termen de 3 luni de la reducerea gradului de secretizare al informaţiilor conţinute de ele.

(3) În cazul majorării gradului de secretizare al informaţiilor, modificarea parafei de secretizare se face imediat.

(4) Decizia de modificare a parafei de secretizare se adoptă de către persoana cu funcţie de răspundere care a secretizat informaţia sau de către succesorul ei de drept. Despre modificarea parafei de secretizare se informează alte autorităţi publice sau persoane juridice cărora le-a fost expediat documentul.

(5) Dacă documentul primit de la o altă autoritate publică sau persoană juridică urmează a fi secretizat sau acestui document i-a fost atribuită incorect parafa de secretizare, atunci destinatarul trebuie să informeze expeditorul imediat, dar nu mai tîrziu de 3 zile de la data înregistrării documentului, expunînd motivele secretizării ori modificării parafei de secretizare. Destinatarul care a înaintat propunerea de secretizare sau de modificare a parafei de secretizare este înştiinţat asupra deciziei luate de către expeditor.

(6) Modificarea parafei de secretizare a documentelor secrete selectate pentru arhivele de stat se efectuează de către arhivele de stat împreună cu autorităţile publice sau cu alte persoane juridice, iar, după caz, cu succesorii lor de drept, ale căror documente se păstrează în arhive.

Articolul 16. Limitarea drepturilor de proprietate
ale persoanelor juridice şi cetăţenilor
asupra informaţiilor în legătură cu
secretizarea lor

(1) Conducătorii autorităţilor publice cu împuterniciri de dispoziţie asupra informaţiilor atribuite la secret de stat sînt în drept să adopte decizii privind secretizarea informaţiilor aflate în proprietatea persoanelor juridice şi a cetăţenilor (în continuare - proprietarul informaţiilor) dacă aceste informaţii sînt atribuite, în modul stabilit, la secret de stat. Informaţiile în cauză sînt secretizate la propunerea proprietarului informaţiilor sau din iniţiativa autorităţii publice interesate.

(2) Prejudiciul material cauzat proprietarului informaţiilor în legătură cu secretizarea lor urmează a fi reparat de către stat în modul stabilit în contractul încheiat între proprietar şi autoritatea publică în dispoziţia căreia trec aceste informaţii. Contractul prevede, de asemenea, obligaţia proprietarului informaţiilor

de a nu le divulga, modul şi condiţiile protecţiei secretului de stat, consimţământul proprietarului informaţiilor privind exercitarea dreptului de proprietate cu restricţiile prevăzute de prezenta lege.

(3) Dacă proprietarul informaţiilor refuză să încheie contract sau încalcă prevederile acestuia, în temeiul unei hotărîri definitive a instanţei de judecată, informaţiile atribuite la secret de stat şi purtătorii lor materiali sînt trecuţi în proprietatea statului, cu condiţia restituirii preliminare şi depline a costului informaţiilor proprietarului. Fostul proprietar este preavizat în scris privind răspunderea pentru divulgarea secretului de stat, prevăzută de legislaţia în vigoare.

(4) Proprietarul informaţiilor este în drept să atace în instanţa de judecată acţiunile persoanelor cu funcţii de răspundere care, în opinia sa, îi lezează drepturile. Dacă instanţa de judecată recunoaşte că acţiunile persoanelor cu funcţii de răspundere sînt nelegitime, modul de reparare a prejudiciului cauzat proprietarului informaţiilor este stabilit printr-o hotărîre a instanţei de judecată, conform legislaţiei.

Articolul 17. Contestarea deciziei de secretizare a informaţiilor

(1) Orice cetăţean sau persoană juridică are dreptul să se adreseze persoanelor cu funcţii de răspundere care au secretizat anumite informaţii cu o cerere motivată privind desecretizarea acestor informaţii. Persoanele cu funcţii de răspundere în cauză sînt obligate, în termen de o lună, să dea un răspuns scris cetăţeanului sau persoanei juridice la această cerere.

(2) Persoanele cu funcţii de răspundere care se eschivează de la examinarea în fond a cererii poartă răspundere conform legislaţiei.

(3) Decizia de secretizare a informaţiilor poate fi contestată la organul sau la persoana cu funcţie de răspundere ierarhic superioară, la Comisia interdepartamentală pentru protecţia secretului de stat sau în instanţa de contencios administrativ. În cazul respingerii cererii înaintate în ordine ierarhică, cetăţeanul sau persoana juridică are dreptul să conteste în instanţa de contencios administrativ decizia organului sau a persoanei cu funcţie de răspundere ierarhic superioară. Dacă una dintre aceste autorităţi recunoaşte secretizarea drept neîntemeiată, informaţiile respective urmează a fi desecretizate în modul stabilit de prezenta lege.

(4) Instanţa de contencios administrativ examinează cererea conform prevederilor Legii contenciosului administrativ nr.793-XIV din 10 februarie 2000.

Articolul 18. Desecretizarea informaţiilor

(1) Drept temei pentru desecretizarea informaţiilor servesc:

a) expirarea termenului de secretizare a informaţiilor;

b) schimbarea circumstanţelor obiective, ca urmare a căreia protecţia ulterioară a anumitor informaţii atribuite la secret de stat devine inoportună;

c) modificarea art.7 şi 8 din prezenta lege, modificarea Nomenclatorului informaţiilor atribuite la secret de stat sau a nomenclatoarelor departamentale de informaţii care urmează a fi secretizate;

d) existenţa unei decizii care constată drept neîntemeiată secretizarea informaţiilor.

(2) Desecretizarea informaţiilor se face de către persoanele cu funcţii de răspundere cu împuterniciri de secretizare a informaţiilor respective.

(3) Comisia interdepartamentală pentru protecţia secretului de stat, precum şi conducătorii autorităţilor publice şi ai altor persoane juridice sînt împuterniciţi să desecretizeze informaţiile care au fost secretizate în mod neîntemeiat de către persoanele cu funcţii de răspundere din subordine.

(4) Conducătorii arhivelor de stat sînt împuterniciţi să desecretizeze purtătorii materiali de informaţii atribuite la secret de stat care se păstrează în fondurile închise ale arhivelor, cu condiţia că organizaţia întemeietoare a fondului sau succesorul ei de drept le deleagă astfel de împuterniciri. În caz de lichidare a organizaţiei întemeietoare a fondului şi de lipsă a succesorului ei de drept, chestiunea desecretizării purtătorilor materiali de informaţii atribuite la secret de stat este examinată de către Comisia interdepartamentală pentru protecţia secretului de stat.

Capitolul IV

Dispunerea de informaţii atribuite la secret de stat

Articolul 19. Transmiterea reciprocă a informaţiilor atribuite la secret de stat între autorităţile publice şi alte persoane juridice

(1) Transmiterea reciprocă a informaţiilor atribuite la secret de stat între autorităţile publice şi alte persoane juridice care nu sînt în raporturi de subordonare şi nu execută lucrări comune se efectuează cu permisiunea autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii.

(2) Autorităţile publice şi alte persoane juridice care solicită furnizarea unor informaţii atribuite la secret de stat sînt obligate să creeze condiţii ce ar asigura protecţia acestor informaţii. Conducătorii lor poartă răspundere personală pentru încălcarea restricţiilor privind familiarizarea cu informaţii atribuite la secret de stat.

(3) Drept condiţie obligatorie de transmitere a informaţiilor atribuite la secret de stat autorităţilor publice este îndeplinirea de către acestea a cerinţelor prevăzute la art.32 alin.(3), iar în cazul celorlalte persoane juridice – prezenţa

certificatului de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor atribuite la secret de stat.

(4) Modul de transmitere reciprocă a informaţiilor atribuite la secret de stat între autorităţile publice şi alte persoane juridice este stabilit de Regulamentul cu privire la asigurarea regimului secret în autorităţile publice şi alte persoane juridice.

Articolul 20. Transmiterea informaţiilor atribuite la secret de stat în legătură cu efectuarea unor lucrări comune şi a altor lucrări

(1) Transmiterea informaţiilor atribuite la secret de stat persoanelor juridice sau cetăţenilor, în legătură cu efectuarea unor lucrări comune şi a altor lucrări, se face de către beneficiarul acestor lucrări, cu permisiunea autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii şi numai în volumul necesar pentru efectuarea lucrărilor respective. Totodată, înainte de a transmite informaţiile atribuite la secret de stat, beneficiarul este obligat să se convingă că persoana juridică dispune de certificat de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor avînd un anumit grad de secretizare, iar cetăţenii – au dreptul de acces la informaţiile atribuite la secret de stat în forma corespunzătoare.

(2) În timpul efectuării lucrărilor comune şi a altor lucrări şi a apariţiei, în legătură cu aceasta, a necesităţii de a utiliza informaţii atribuite la secret de stat, persoanele juridice, inclusiv cele cu capital privat, pot încheia cu alte persoane juridice care dispun de certificat de securitate contracte de folosire a serviciilor prestate de către subdiviziunile lor de protecţie a informaţiilor atribuite la secret de stat, fapt ce se notifică în certificatul de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor atribuite la secret de stat.

(3) Contractul pentru efectuarea lucrărilor comune şi a altor lucrări, încheiat în modul stabilit de lege, prevede obligaţiile reciproce ale părţilor de a asigura integritatea informaţiilor atribuite la secret de stat atît în procesul efectuării lucrărilor, cît şi după încheierea lor, precum şi condiţiile de finanţare a lucrărilor (serviciilor) de protecţie a secretului de stat.

(4) Dacă în timpul efectuării lucrărilor comune şi a altor lucrări executantul încalcă obligaţiile de protecţie a secretului de stat, beneficiarul are dreptul să suspende executarea comenzii pînă la lichidarea încălcărilor, iar în cazul încălcărilor repetate – să solicite anularea comenzii şi a certificatului de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor atribuite la secret de stat şi tragerea la răspundere a persoanelor vinovate. Prejudiciul material cauzat de către executant statului, în persoana beneficiarului, urmează a fi reparat conform legislaţiei.

(5) Modul de transmitere a informaţiilor atribuite la secret de stat în legătură cu efectuarea unor lucrări comune şi a altor lucrări este stabilit de Regulamentul cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor

persoane juridice.

Articolul 21. Transmiterea informaţiilor atribuite la secret

de stat altor state sau organizaţiilor internaţionale

(1) Pentru a fi adoptată decizia privind transmiterea informaţiilor atribuite la secret de stat altor state sau organizaţiilor internaţionale, autoritatea publică prezintă Comisiei interdepartamentale pentru protecţia secretului de stat o propunere motivată, avizată de către Serviciul de Informaţii şi Securitate şi de autoritatea publică cu împuterniciri de dispoziţie asupra acestor informaţii.

(2) Comisia interdepartamentală pentru protecţia secretului de stat adoptă o concluzie de expertiză privind posibilitatea şi oportunitatea transmiterii informaţiilor atribuite la secret de stat.

(3) Decizia privind transmiterea informaţiilor atribuite la secret de stat altor state sau organizaţiilor internaţionale se adoptă de Guvern în baza concluziei de expertiză a Comisiei interdepartamentale pentru protecţia secretului de stat, dacă tratatele internaţionale la care Republica Moldova este parte nu prevăd altfel.

(4) Obligaţiile părţii care primeşte informaţiile atribuite la secret de stat privind protecţia acestora sînt stipulate în acordul (contractul) încheiat.

Capitolul V

Protecţia secretului de stat

Articolul 22. Organele de protecţie a secretului de stat

(1) Organele de protecţie a secretului de stat sînt:

a) Comisia interdepartamentală pentru protecţia secretului de stat;

b) Serviciul de Informaţii şi Securitate;

c) autorităţile publice şi alte persoane juridice şi subdiviziunile lor de protecţie a informaţiilor atribuite la secret de stat.

(2) Comisia interdepartamentală pentru protecţia secretului de stat este un organ colegial care coordonează activitatea autorităţilor publice în domeniul protecţiei secretului de stat. Comisia interdepartamentală îşi exercită atribuţiile potrivit unui regulament aprobat de Guvern.

(3) Serviciul de Informaţii şi Securitate organizează şi asigură protecţia secretului de stat conform atribuţiilor ce îi revin şi potrivit legislaţiei şi tratatelor internaţionale la care Republica Moldova este parte.

(4) Autorităţile publice şi alte persoane juridice asigură protecţia secretului de stat conform sarcinilor ce le revin şi în limitele competenţelor lor. De asigu-

rarea protecţiei secretului de stat în cadrul autorităţilor publice şi al altor persoane juridice răspund conducătorii acestora. În funcţie de volumul lucrărilor cu utilizarea informaţiilor atribuite la secret de stat, conducătorii autorităţilor publice şi ai altor persoane juridice formează subdiviziuni de protecţie a informaţiilor atribuite la secret de stat şi le stabilesc atribuţiile în conformitate cu Regulamentul privind asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice, ţinînd cont de specificul lucrărilor efectuate.

Articolul 23. Condiţiile de păstrare a purtătorilor materiali

de informaţii atribuite la secret de stat

(1) Condiţiile de păstrare a purtătorilor materiali de informaţii atribuite la secret de stat se stabilesc prin Regulamentul cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice.

(2) În funcţie de specificul activităţii autorităţii publice şi a altor persoane juridice şi în conformitate cu condiţiile menţionate la alin.(1), conducătorii acestora pot stabili condiţii speciale de păstrare a purtătorilor materiali de informaţii atribuite la secret de stat.

Articolul 24. Perfectarea şi reperfectarea dreptului

de acces la secretul de stat

(1) Perfectarea dreptului de acces la secretul de stat al cetăţenilor Republicii Moldova se realizează în mod benevol, potrivit cu Regulamentul cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice, şi prevede:

a) stabilirea necesităţii de a lucra cu informaţii atribuite la secret de stat;

b) consimţămîntul scris al cetăţeanului pentru aplicarea măsurilor de verificare din partea organelor competente;

c) verificarea cetăţeanului în legătură cu perfectarea (reperfectarea) dreptului de acces la secretul de stat;

d) asumarea în scris de către cetăţean a obligaţiei privind păstrarea secretului de stat care îi va fi încredinţat;

e) acordul scris al cetăţeanului pentru limitarea drepturilor sale în legătură cu accesul la secretul de stat, prevăzută de prezenta lege;

f) familiarizarea cetăţeanului, contra semnătură, cu normele ce prevăd răspunderea pentru încălcarea legislaţiei privind secretul de stat;

g) determinarea tipurilor, mărimii şi a modului de acordare a compensaţiilor în legătură cu efectuarea lucrărilor legate de accesul la secretul de stat;

h) luarea deciziei de către conducătorul autorităţii publice sau al altei persoane juridice privind acordarea dreptului de acces la secretul de stat.

(2) În funcţie de gradul de secretizare a informaţiilor sînt stabilite:

a) următoarele forme de acces la secretul de stat:

- forma 1 – pentru lucrul cu informaţii atribuite la secret de stat avînd gradele de secretizare „Strict secret", „Secret", „Confidenţial" şi „Restricţionat";

- forma 2 – pentru lucrul cu informaţii atribuite la secret de stat avînd gradele de secretizare „Secret", „Confidenţial" şi „Restricţionat";

- forma 3 – pentru lucrul cu informaţii atribuite la secret de stat avînd gradul de secretizare „Confidenţial" şi „Restricţionat";

- forma 4 – pentru lucrul cu informaţii atribuite la secret de stat avînd gradul de secretizare „Restricţionat";

b) şi următoarele termene pentru care se perfectează dreptul de acces la secretul de stat:

- pentru forma 1 – 5 ani;

- pentru forma 2 – 7 ani;

- pentru forma 3 – 9 ani;

- pentru forma 4 – 12 ani.

(3) Durata dreptului de acces la secretul de stat nu poate depăşi durata atribuţiilor care au servit drept temei pentru acordarea acestuia.

(4) Dreptul de acces la secretul de stat se acordă cetăţenilor Republicii Moldova cu capacitatea de exerciţiu deplină, începînd cu vîrsta de 18 ani, care solicită acest drept în legătură cu activitatea lor de serviciu, de producere, ştiinţifico-teoretică, sau în legătură cu studiile, printr-un ordin sau dispoziţie scrisă a conducătorului autorităţii publice sau al altei persoane juridice în care acest cetăţean lucrează, îşi îndeplineşte serviciul sau studiază.

(5) Dreptul de acces la secretul de stat i se acordă conducătorului autorităţii publice sau al altei persoane juridice printr-un ordin sau dispoziţie scrisă a persoanei cu funcţie de răspundere care îl numeşte în funcţie, iar în cazul în care autoritatea publică sau persoana juridică nu este subordonată altei autorităţi publice sau altei persoane juridice ori nu intră în domeniul lor de administrare, dreptul de acces la secretul de stat se acordă prin ordinul sau dispoziţia scrisă a conducătorului autorităţii publice sau al altei persoane juridice care este beneficiară a lucrărilor legate de secretul de stat.

(6) Dacă solicitarea cetăţeanului de a dispune de informaţii atribuite la secret de stat nu este legată de locul său de muncă, de serviciu sau de studii, dreptul de acces la secretul de stat poate fi acordat

(7) Decizia de acordare a dreptului de acces la secretul de stat este luată în termen de 5 zile de la primirea de către autoritatea publică sau altă persoană

juridică a încheierii asupra materialelor verificării cetăţeanului în legătură cu perfectarea dreptului de acces la secretul de stat.

(8) Obligaţiile reciproce ale administraţiei şi ale persoanei căreia i se perfectează dreptul de acces la secretul de stat se stipulează în contractul de angajare în muncă (în serviciu).

(9) Reperfectarea dreptului de acces la secretul de stat se face în cazurile:

a) expirării termenului pentru care a fost perfectat acest drept, dacă este necesar să se lucreze în continuare cu informaţii atribuite la secret de stat;

b) perfectării unei alte forme de acces la secretul de stat în legătură cu necesitatea de a lucra cu informaţii atribuite la secret de stat cu un grad mai înalt de secretizare.

(10) Fiecare dintre autorităţile publice sau alte persoane juridice care lucrează cu secrete de stat trebuie să ţină un registru privind personalul său cu drept de acces la secretul de stat.

(11) În activitatea cu utilizarea secretelor interstatale, la realizarea colaborărilor pot fi atraşi savanţi, specialişti, traducători, lucrători tehnici şi alţi specialişti care, conform legislaţiei în vigoare a statului lor, au acces la secretele de stat.

Articolul 25. Refuzul de acordare a dreptului de acces la secretul de stat

(1) Dreptul de acces la secretul de stat îi este refuzat cetăţeanului în cazurile:

a) în care acesta nu expune o necesitate motivată de a lucra cu informaţii atribuite la secret de stat;

b) sprijinirii de către acesta a activităţii unui stat străin, a unei organizaţii străine sau a reprezentanţilor acestora, precum şi a unor cetăţeni străini sau apatrizi ce cauzează prejudicii intereselor şi/sau securităţii Republicii Moldova sau în cazul participării cetăţeanului la activitatea unor partide sau asociaţii obşteşti a căror activitate este suspendată, limitată sau interzisă în modul stabilit de lege;

c) descoperirii, în urma măsurilor de verificare, a altor acţiuni ale acestuia care prezintă pericol pentru securitatea Republicii Moldova;

d) refuzului acestuia de a-şi da consimţământul scris pentru aplicarea măsurilor de verificare din partea organelor competente, pentru limitarea drepturilor sale în legătură cu accesul la secretul de stat, prevăzută de prezenta lege, sau refuzului de a-şi asuma obligaţia scrisă privind păstrarea secretului de stat ce îi va fi încredinţat;

e) prezenţei la acesta a antecedentelor penale pentru infracţiuni săvîrşite cu intenţie, aflării acestuia sub urmărire penală sau al limitării de către instanţa de judecată a capacităţii sale de exerciţiu;

f) depunerii la autoritatea publică competentă a cererii de renunţare la cetăţenia Republicii Moldova;

h) prezenţei la acesta a unor contraindicaţii medicale pentru lucrul cu informaţiile atribuite la secret de stat, conform nomenclatorului aprobat de Ministerul Sănătății, Muncii și Protecției Sociale;

i) comunicării de către cetăţean a unor date incomplete sau neautentice la perfectarea dreptului de acces la secretul de stat;

j) domicilierii permanente a cetăţeanului peste hotare sau al perfectării documentelor pentru plecarea cu traiul permanent într-o altă ţară;

k) neexecutării de către cetăţean a obligaţiilor privind păstrarea secretului de stat care i-a fost încredinţat.

(2) Decizia privind refuzul de a acorda dreptul de acces la secretul de stat se adoptă de către conducătorul autorității publice sau al altei persoane juridice ţinîndu-se cont de rezultatele verificării fiecărui cetăţean în parte, se comunică în scris cetăţeanului şi poate fi atacată în organul ierarhic superior sau în instanţa de judecată.

Articolul 26. Verificarea cetăţenilor în legătură cu
perfectarea (reperfectarea) dreptului
de acces la secretul de stat

(1) Verificarea cetăţenilor în legătură cu perfectarea (reperfectarea) dreptului de acces la secretul de stat se efectuează de către Serviciul de Informaţii şi Securitate, în termen de o lună, în modul stabilit de prezenta lege şi de Legea privind activitatea operativă de investigaţii. Numărul măsurilor de verificare este în dependenţă directă de gradul de secretizare al informaţiilor la care va avea acces persoana.

(2) În cadrul verificării, Serviciul de Informaţii şi Securitate stabileşte prezenţa sau lipsa circumstanţelor prevăzute la art.25 alin.(1) lit.b), c), f), g), i), j) şi k).

(3) Prezenţa sau lipsa circumstanţelor prevăzute la art.25 alin.(1) lit.a), d), e) şi h) se stabileşte de către autoritatea publică sau o altă persoană juridică care perfectează dreptul cetăţeanului de acces la secretul de stat.

(4) Concluzia Serviciului de Informaţii şi Securitate privind imposibilitatea de a acorda cetăţeanului dreptul de acces la secretul de stat este executorie pentru persoanele cu funcţii de răspundere împuternicite să adopte decizia privind acordarea dreptului de acces la secretul de stat, însă nu exclude o solicitare repetată în cazul înlăturării împrejurărilor care fac imposibilă acordarea dreptului de acces la secretul de stat.

(5) Nu se admite numirea (angajarea) cetăţeanului într-o funcţie care implică

lucrul cu informaţii atribuite la secretul de stat sau accesul la secretul de stat înainte de prezentarea concluziei asupra materialelor verificării cetăţeanului.

Articolul 27. Suspendarea şi încetarea dreptului
de acces la secretul de stat

(1) Dreptul de acces la secretul de stat este suspendat în cazurile:

a) punerii sub învinuire a cetăţeanului pentru săvîrşirea unei infracţiuni incompatibile cu activitatea ce presupune utilizarea informaţiilor atribuite la secret de stat, pînă la pronunţarea unei hotărîri judecătoreşti definitive şi irevocabile;

b) iniţierii unei investigaţii de serviciu în legătură cu încălcarea obligaţiei de nedivulgare a secretului de stat, pînă la terminarea investigaţiei şi adoptarea unei decizii definitive, dar nu pentru mai mult de 30 de zile.

(2) Dreptul de acces la secretul de stat poate fi suspendat în cazul necesităţii efectuării unei verificări suplimentare în legătură cu posibila apariţie a circumstanţelor prevăzute la art.25, pînă la terminarea verificării, dar nu mai mult de 30 de zile.

(3) Dreptul de acces la secretul de stat încetează în cazurile:

a) apariţiei sau descoperirii circumstanţelor prevăzute la art.25;

b) eliberării din funcţia (încetării contractului individual de muncă) care implică lucrul cu informaţii atribuite la secret de stat;

c) încălcării, chiar şi o singură dată, a obligaţiilor prevăzute în contractul individual de muncă ce ţin de protecţia secretului de stat;

d) pierderii cetăţeniei Republicii Moldova.

(4) Decizia privind suspendarea sau încetarea dreptului de acces la secretul de stat se adoptă de către persoana cu funcţie de răspundere împuternicită să adopte decizia privind acordarea acestui drept şi poate fi atacată în organul ierarhic superior sau în instanţa de contencios administrativ.

(5) Cetăţeanul al cărui drept de acces la secretul de stat a încetat, dacă îndeplinirea obligaţiilor lui funcţionale necesită acest drept, în modul prevăzut de legislaţia muncii, urmează să fie transferat la un alt loc de muncă (la o altă funcţie), care nu are nici o legătură cu informaţiile atribuite la secret de stat, iar în cazul imposibilităţii transferului, urmează a fi concediat (eliberat din funcţie) conform legislaţiei în vigoare.

(6) Suspendarea sau încetarea dreptului de acces la secretul de stat nu eliberează cetăţeanul de obligaţiile asumate privind nedivulgarea secretului de stat.

(7) Modul de perfectare, reperfectare şi încetare a dreptului de acces la secretul de stat se stabileşte în Regulamentul cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice.

Articolul 28. Modul special de acces la secretul de stat

(1) Titularii funcţiilor prevăzute în anexa nr. 1 au dreptul de acces la secretul de stat de forma 1 şi 2 de la numirea (alegerea) lor în funcţie, doar după întocmirea unei obligaţii scrise privind nedivulgarea secretului de stat.

(1^1) Dreptul de acces la secretul de stat pentru titularii funcţiilor prevăzute în anexa nr. 1 poate fi suspendat sau încetează în condiţiile generale stabilite de prezenta lege.

(2) Prevederile alin.(1) nu se aplică persoanelor care deţin cetăţenia altui stat.

(3) Modul de acces la secretul de stat în cazul declarării stării de urgenţă, de asediu sau de război poate fi modificat prin hotărîre de Guvern.

(4) Accesul cetăţenilor străini şi al apatrizilor la secretul de stat se acordă în cazuri excepţionale în temeiul tratatelor internaţionale la care Republica Moldova este parte sau în temeiul dispoziţiei scrise a Prim-ministrului, adoptată în baza propunerilor Comisiei interdepartamentale pentru protecţia secretului de stat, ţinînd cont de necesitatea asigurării intereselor şi/sau securităţii Republicii Moldova.

Articolul 29. Obligaţiile cetăţeanului privind nedivulgarea secretului de stat

Cetăţeanul căruia i s-a perfectat dreptul de acces la secretul de stat este obligat:

a) să nu admită divulgarea, prin orice metodă, a secretului de stat care i-a fost încredinţat sau i-a devenit cunoscut în legătură cu îndeplinirea obligaţiilor funcţionale;

b) să nu participe la acţiunile partidelor şi asociaţiilor obşteşti a căror activitate a fost suspendată, limitată sau interzisă în modul stabilit de lege;

c) să nu sprijine activitatea unui stat străin, a unei organizaţii străine sau a reprezentanţilor acestora, precum şi a cetăţenilor străini şi apatrizilor ce cauzează prejudicii intereselor şi/sau securităţii Republicii Moldova;

d) să execute cerinţele asigurării regimului secret;

e) să comunice persoanei cu funcţie de răspundere care i-a acordat dreptul de acces la secretul de stat şi subdiviziunii de protecţie a informaţiilor atribuite la secret de stat despre apariţia circumstanţelor prevăzute la art.25 sau a altor împrejurări ce împiedică păstrarea secretului de stat care i-a fost încredinţat, precum şi despre ieşirea sa de pe teritoriul Republicii Moldova;

f) să respecte alte prevederi ale legislaţiei privind secretul de stat.

Articolul 30. Restrîngerea exerciţiului unor drepturi
ale cetăţeanului în legătură cu dreptul
de acces şi accesul la secretul de stat

Restrîngerea exerciţiului unor drepturi ale cetăţeanului în legătură cu dreptul de acces şi accesul la secretul de stat se poate referi la:

a) restricţii de utilizare a descoperirilor şi invenţiilor ce conţin informaţii atribuite la secret de stat şi de răspîndire a acestor informaţii;

b) restrîngerea dreptului la inviolabilitatea vieţii private în timpul efectuării măsurilor de control în perioada perfectării (reperfectării) dreptului de acces la secretul de stat.

Articolul 31. Compensaţiile acordate cetăţenilor
în legătură cu efectuarea lucrărilor
legate de accesul la secretul de stat

(1) În cazul în care, în virtutea activităţii sale profesionale, cetăţeanul lucrează permanent cu informaţii atribuite la secret de stat, acestuia i se stabileşte un spor la salariu în funcţie de gradul de secretizare a informaţiilor la care are acces.

(2) Colaboratorilor subdiviziunilor de protecţie a informaţiilor atribuite la secret de stat, suplimentar la sporul prevăzut la alin.(1), li se stabilesc sporuri la salariu pentru vechimea în muncă (în serviciu) în cadrul acestor subdiviziuni.

(3) Mărimile şi modul de acordare a sporurilor prevăzute la alin.(1) şi (2), precum şi alte tipuri de compensaţii acordate cetăţenilor care lucrează în condiţii de regim secret se stabilesc de Guvern.

Articolul 32. Certificatul de securitate pentru
efectuarea lucrărilor cu utilizarea
informaţiilor atribuite la secret de stat

(1) Activitatea persoanelor juridice, exceptînd autorităţile publice, ce ţine de utilizarea informaţiilor atribuite la secret de stat, crearea mijloacelor de protejare a informaţiei, realizarea măsurilor şi/sau prestarea serviciilor de protecţie a secretului de stat se desfăşoară în baza certificatului de securitate eliberat de Comisia interdepartamentală pentru protecţia secretului de stat în modul stabilit de prezenta lege.

(2) Certificatul de securitate se eliberează după efectuarea unei expertize speciale a persoanei juridice privind existenţa condiţiilor pentru desfăşurarea activităţii legate de secretul de stat şi după atestarea conducătorului ei. Atestarea conducătorului persoanei juridice se efectuează în modul stabilit de Regula-

mentul cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice.

(3) Certificatul de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor atribuite la secret de stat se eliberează persoanei juridice cu condiţia că ea:

a) trebuie să execute lucrările menţionate în conformitate cu actele normative, competenţa, sarcinile, comenzile sau acordurile (contractele) de stat;

b) dispune de o încăpere pentru efectuarea lucrărilor cu utilizarea informaţiilor atribuite la secret de stat, locuri de păstrare a documentelor secrete şi a altor purtători materiali de informaţii atribuite la secret de stat, care corespund cerinţelor de asigurare a caracterului secret al lucrărilor menţionate, exclud posibilitatea accesului la ele al persoanelor neautorizate, garantează păstrarea purtătorilor materiali de informaţii atribuite la secret de stat;

c) respectă cerinţele legislaţiei privind regimul secret al lucrărilor şi al altor acţiuni legate de utilizarea informaţiilor atribuite la secret de stat, privind modul de perfectare a dreptului de acces la secretul de stat şi de organizare a accesului la informaţiile atribuite la secret de stat, de primire a cetăţenilor străini, de utilizare a cifrurilor de stat şi a mijloacelor criptografice etc.;

d) dispune de subdiviziuni de protecţie a informaţiilor atribuite la secret de stat şi/sau de colaboratori special pregătiţi pentru activitatea de protecţie a secretului de stat;

e) dispune de mijloace certificate de protejare a informaţiilor.

(4) Certificatul de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor atribuite la secret de stat se eliberează fără taxă, pe o durată nedeterminată.

Articolul 33. Protecţia secretului de stat în caz
de schimbare a funcţiilor subiecţilor
raporturilor juridice

(1) În caz de reorganizare sau lichidare fie de încetare a lucrărilor cu utilizarea informaţiilor atribuite la secret de stat, autorităţile publice şi alte persoane juridice care deţin informaţii atribuite la secret de stat sînt obligate să întreprindă măsuri pentru asigurarea protecţiei acestor informaţii şi a purtătorilor lor materiali.

(2) Purtătorii materiali de informaţii atribuite la secret de stat se distrug, se predau spre păstrare la arhivă sau se transmit în modul stabilit:

a) succesorului de drept al autorităţii publice sau al altei persoane juridice deţinătoare de informaţii atribuite la secret de stat, în cazul în care acest succesor dispune de împuterniciri (certificat de securitate) pentru efectuarea lucrări-

lor cu utilizarea acestor informaţii;

b) autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii;

c) altei autorităţi publice sau persoane juridice, la decizia Comisiei interdepartamentale pentru protecţia secretului de stat.

Articolul 34. Protecţia secretului de stat

în cadrul şedinţelor judiciare

Cauzele penale, civile şi cele de contencios administrativ în cadrul cărora sînt prezentate informaţii atribuite la secret de stat se examinează în şedinţă închisă, cu respectarea regulilor de procedură, precum şi a prevederilor prezentei legi.

Articolul 35. Protejarea tehnică şi criptografică

a informaţiilor atribuite la secret de stat.

Certificarea mijloacelor de protejare a

informaţiilor atribuite a secret de stat

(1) Protejarea tehnică şi criptografică a informaţiilor atribuite la secret de stat se efectuează în modul stabilit de Regulamentul cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice.

(2) Mijloacele de protejare a informaţiilor atribuite la secret de stat trebuie să dispună de certificat privind corespunderea lor cu cerinţele de protecţie a informaţiilor avînd gradul corespunzător de secretizare.

(3) Organizarea şi coordonarea certificării şi expertizei mijloacelor de protejare a informaţiilor atribuite la secret de stat revin Serviciului de Informaţii şi Securitate. Certificarea se efectuează conform actelor normative în domeniu şi standardelor naţionale ale Republicii Moldova.

(4) Certificarea mijloacelor de protejare criptografică şi tehnică a secretului de stat se efectuează fără taxă, pe o durată nedeterminată.

Articolul 36. Finanţarea măsurilor de protecţie

a secretului de stat

(1) Activitatea autorităţilor publice, a altor persoane juridice finanţate din bugetul de stat şi bugetele unităţilor administrativ-teritoriale, precum şi a subdiviziunilor lor de protecţie a informaţiilor atribuite la secret de stat, se finanţează de la bugetele respective, iar activitatea celorlalte persoane juridice – din mijloacele proprii.

(2) Controlul asupra cheltuielilor financiare pentru realizarea măsurilor de protecţie a secretului de stat îl exercită conducătorii autorităţilor publice şi ai altor persoane juridice, subdiviziunile lor de control financiar intern, precum

şi reprezentanţi special împuterniciţi ai Curţii de Conturi şi ai Ministerului Finanţelor. Dacă acest control implică accesul la secretul de stat, persoanele menţionate trebuie să posede dreptul de acces la informaţii avînd gradul de secretizare corespunzător.

Capitolul VI
Controlul privind asigurarea protecţiei secretului de stat şi răspunderea pentru încălcarea legislaţiei cu privire la secretul de stat

Articolul 37. Controlul privind asigurarea protecţiei secretului de stat

(1) Controlul privind asigurarea protecţiei secretului de stat se efectuează în scopul studierii şi aprecierii stării reale privind păstrarea secretelor de stat, al depistării neajunsurilor şi încălcărilor regimului secret, al constatării cauzelor apariţiei acestor neajunsuri şi elaborării propunerilor în vederea prevenirii şi lichidării acestora.

(2) Conducătorii autorităţilor publice şi ai altor persoane juridice, precum şi subdiviziunile lor de protecţie a informaţiilor atribuite la secret de stat sînt obligaţi să exercite controlul permanent privind asigurarea protecţiei informaţiilor respective deţinute de ele sau de persoanele juridice din subordine.

(3) Serviciul de Informaţii şi Securitate este abilitat să efectueze controlul privind starea protecţiei secretului de stat în cadrul autorităţilor publice şi al altor persoane juridice. Concluziile Serviciului de Informaţii şi Securitate, întocmite în baza rezultatelor controlului, sînt obligatorii spre executare pentru persoanele cu funcţii de răspundere ale autorităţilor publice şi ale altor persoane juridice.

(4) Serviciul de Informaţii şi Securitate este obligat să informeze Parlamentul asupra constatărilor şi concluziilor rezultate din activitatea desfăşurată pentru protecţia secretului de stat.

(5) Controlul privind asigurarea protecţiei secretului de stat în aparatele Parlamentului, Preşedintelui Republicii Moldova şi Guvernului este organizat de către conducătorii acestor organe.

(6) Autorităţile publice şi alte persoane juridice, în calitate de beneficiari ai lucrărilor cu utilizarea informaţiilor atribuite la secret de stat, sînt obligate să controleze starea protecţiei acestor informaţii transmise antreprenorilor în legătură cu executarea comenzilor.

Articolul 38. Răspunderea pentru încălcarea legislaţiei cu privire la secretul de stat

(1) Persoanele vinovate de încălcarea prezentei legi poartă răspundere penală, civilă, administrativă sau disciplinară conform legislaţiei.

(2) Persoanele cu funcţii de răspundere având împuterniciri de dispoziţie asupra informaţiilor atribuite la secret de stat poartă răspundere penală, civilă, administrativă sau disciplinară, conform legislaţiei, pentru atribuirea neîntemeiată a informaţiilor la secret de stat, pentru neluarea intenţionată a deciziei privind atribuirea informaţiilor la secret de stat, a căror divulgare poate cauza prejudicii intereselor şi/sau securităţii statului, precum şi pentru luarea unor decizii neîntemeiate privind excluderea din nomenclatorul departamental a informaţiilor atribuite la secret de stat.

Articolul 38[1]. Licențierea activității de protecție a informației

care nu este atribuită la secret de stat

(1) Licenţierea activităţii de protecţie a informației care nu este atribuită la secret de stat se efectuează în conformitate cu Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător în partea în care nu este reglementată de prezenta lege.

(2) Licenţa pentru activitatea de protecţie a informației poate fi eliberată, la cererea solicitantului, pentru una sau mai multe dintre următoarele activități specifice:

a) importul, exportul, proiectarea, producerea şi comercializarea mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informației (cu excepția activității desfăşurate de către autoritățile publice învestite cu acest drept prin lege);

b) prestarea serviciilor în domeniul protecției criptografice a informației (cu excepția activității în domeniul protecției secretului de stat);

c) prestarea serviciilor în domeniul protecției tehnice a informației (cu excepția activității în domeniul protecției secretului de stat).

(3) Pentru obținerea sau prelungirea licenței, solicitantul depune la Agenția Servicii Publice:

a) cererea care să conțină: denumirea, forma juridică de organizare, IDNO-ul întreprinderii sau al organizației ori numele, prenumele, adresa şi IDNP-ul persoanei fizice solicitante; genul de activitate pentru care se solicită licență; asumarea pe propria răspundere de către solicitantul de licență a responsabilității pentru respectarea condițiilor de licențiere la desfăşurarea genului de activitate pentru care se solicită licența și pentru autenticitatea documentelor prezentate;

b) copia de pe titlul de proprietate sau de pe contractul de locaţiune a imobilului unde se va desfăşura activitatea licenţiată;

c) copiile de pe actele de studii ale specialiştilor în domeniu.

(4) La data înregistrării cererii şi documentelor stabilite de prezentul articol pentru eliberarea/prelungirea licenței, autoritatea de licențiere va înştiința Serviciul de Informaţii şi Securitate pentru a se asigura de corespunderea condițiilor de activitate a solicitantului cu cerințele stabilite, a solicita şi a obține autorizațiile necesare desfăşurării activității/activităților solicitate.

(5) În termen de cel mult 10 zile lucrătoare de la data înştiinţării, Serviciul de Informaţii şi Securitate va transmite autorității emitente autorizația sau procesul-verbal de control privind rezultatele verificării efectuate, precum şi copia de pe autorizația emisă în urma controlului. În cazul în care Serviciul de Informaţii şi Securitate nu a transmis autorizația sau nu a inițiat un control în urma înştiinţării şi nu a eliberat procesul-verbal de control în termen de 10 zile lucrătoare de la data înştiinţării, survine principiul aprobării tacite.

(6) În cazul primirii refuzului de a emite autorizație de la Serviciul de Informaţii şi Securitate, autoritatea de licențiere este în drept să refuze eliberarea licenței.

(7) Suspendarea, retragerea şi reperfectarea licenţei se efectuează în conformitate cu Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător.

(8) Licența se eliberează pe un termen de 5 ani.

(9) Condițiile de licențiere, lista documentelor ce se anexează la cererea de eliberare/prelungire a licenței, serviciile ce pot fi prestate în baza licenței, pentru activități specifice, sînt prevăzute în anexele nr. 2, 3 şi 4.

Anexa 1

LISTA
funcţiilor ai căror titulari au dreptul de acces la secretul de stat de forma 1 şi 2

I. Funcţiile ai căror titulari au dreptul de acces la secretul de stat de forma 1

1. Preşedinte al Republicii Moldova
2. Preşedinte al Parlamentului
3. Deputat în Parlament
4. Prim-ministru
5. Membru al Guvernului
6. Secretar general al Guvernului
7. Secretar general al Aparatului Preşedintelui Republicii Moldova
8. Secretar general al Parlamentului
9. Preşedinte al Curţii Constituţionale
10. Preşedinte al Consiliului Superior al Magistraturii
11. Preşedinte al Consiliului Superior al Procurorilor
12. Preşedinte al instanţei judecătoreşti
13. Procuror General
14. Director al Serviciului de Informaţii şi Securitate
15. Director al Serviciului de Protecţie şi Pază de Stat
16. Director al Centrului Naţional Anticorupţie
17. Guvernator al Băncii Naţionale a Moldovei
18. Preşedinte al Curţii de Conturi
19. Preşedinte al Comisiei Naţionale a Pieţei Financiare
20. Preşedinte al Autorităţii Naţionale de Integritate
21. Director general al Serviciului de Stat de Arhivă
22. Conducător al Agenţiei Rezerve Materiale
23. Preşedinte al Consiliului Concurenţei
24. Director al Serviciului Prevenirea şi Combaterea Spălării Banilor

II. Funcţiile ai căror titulari au dreptul de acces la secretul de stat de forma 2

1. Preşedinte al Comisiei Electorale Centrale

2. Preşedinte al Consiliului Coordonator al Audiovizualului

3. Preşedinte al Consiliului pentru prevenirea şi eliminarea discriminărilor şi asigurarea egalităţii

4. Director general al Agenţiei Naţionale pentru Reglementare în Energetică

5. Director al Agenţiei Naţionale pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei

6. Director al Centrului Naţional pentru Protecţia Datelor cu Caracter Personal

7. Director general al Agenţiei Naţionale pentru Siguranţa Alimentelor

8. Avocat al Poporului

9. Avocat al Poporului pentru drepturile copilului

10. Preşedinte al raionului

11. Conducător al autorităţii administrative centrale subordonate Guvernului.

12. Şef al Aparatului Consiliului Superior al Procurorilor.

[Anexa nr.1 modificată prin LP265 din 23.11.18, MO1-5/04.01.19 art.8; în vigoare 04.01.19]

Anexa nr. 2

REGULAMENTUL
privind licenţierea activităţii de prestare a serviciilor
în domeniul importului, exportului, proiectării, producerii
şi comercializării mijloacelor tehnice speciale destinate
pentru obţinerea ascunsă a informaţiei

I. DISPOZIŢII GENERALE

1. Prezentul regulament reglementează activitatea de import, export, proiectare, producere şi comercializare a mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei.

2. La mijloace tehnice speciale destinate pentru obţinerea ascunsă a informaţiei (în continuare – mijloace tehnice speciale) sînt atribuite mijloacele tehnice şi/sau de program proiectate, modificate sau programate pentru captarea, obţinerea, interceptarea, culegerea, ascultarea, înregistrarea şi transmiterea semnalelor informaţionale de natură sonoră, vizuală, electromagnetică sau de altă natură, inclusiv din reţelele de comunicaţii electronice, în scopul obţinerii accesului ascuns la informaţia străină.

3. Activitatea de import, export, proiectare, producere şi comercializare a mijloacelor tehnice speciale poate fi desfăşurată exclusiv de către:

a) autorităţile împuternicite prin lege să desfăşoare activitatea specială de investigaţii;

b) persoanele juridice cu sediul în Republica Moldova, care deţin licenţă de activitate în domeniu.

4. Activitatea de import, export, proiectare, producere şi comercializare a mijloacelor tehnice speciale este realizată doar pentru organele abilitate să exercite activitatea specială de investigaţii.

Se interzice utilizarea mijloacelor tehnice speciale de către persoanele fizice şi juridice care nu sînt împuternicite în acest sens prin lege.

5. Verificarea corespunderii solicitantului de licenţă şi controlul privind respectarea de către titularul de licenţă a condiţiilor de licenţiere pentru activitatea de import, export, proiectare, producere şi comercializare a mijloacelor tehnice speciale se efectuează de către Agenţia Servicii Publice în comun cu Serviciul de Informaţii şi Securitate.

6. Organele vamale vor autoriza plasarea mijloacelor tehnice speciale în regim vamal de import/export doar după prezentarea licenţei şi, după caz, a autorizaţiei respective de către titularul de licenţă.

II. CONDIŢIILE DE DESFĂŞURARE A ACTIVITĂŢII LICENŢIATE DE IMPORT, EXPORT, PROIECTARE, PRODUCERE ŞI COMERCIALIZARE A MIJLOACELOR TEHNICE SPECIALE

7. În scopul desfăşurării activităţii de import, export, proiectare, producere şi comercializare a mijloacelor tehnice speciale, titularii de licenţă trebuie să respecte următoarele condiţii:

a) desfăşurarea activităţii licenţiate în conformitate cu cadrul legislativ şi normativ;

b) dispunerea în proprietate sau în locaţiune a unui imobil, unde se va desfăşura activitatea licenţiată, dotat cu mijloace tehnice de pază şi de păstrare a mijloacelor tehnice speciale, inclusiv a documentaţiei tehnice;

c) deţinerea încăperilor separate destinate pentru oficiu, atelier de producţie, depozit etc.;

d) deţinerea, după caz, a echipamentelor moderne pentru proiectarea şi producerea mijloacelor tehnice speciale;

e) dispunerea de a cel puţin 2 colaboratori, angajaţi permanenţi, cu studii tehnice superioare sau speciale, competenţi în domeniu;

f) elaborarea, în termen de o lună de la eliberarea licenţei, a regulamentului intern, care va stabili condiţiile de organizare a activităţii în domeniul licenţiat, modul de evidenţă, păstrare, comercializare, transmitere şi distrugere a mijloacelor tehnice speciale şi a documentaţiei tehnice; g) organizarea regimului intern într-un mod care să excludă posibilitatea accesului fizic neautorizat la mijloacele tehnice speciale;

h) ţinerea evidenţei mijloacelor tehnice speciale la etapa proiectării, producerii, păstrării, precum şi în timpul efectuării testărilor. Comercializarea sau predarea acestor mijloace beneficiarului, precum şi distrugerea acestora vor fi documentate;

i) asigurarea regimului de confidenţialitate în activitatea licenţiată. Informaţia privind importul, exportul, proiectarea, producerea şi comercializarea mijloacelor tehnice speciale poate fi prezentată doar organelor abilitate să exercite activitatea specială de investigaţii, Comisiei republicane de expertiză a mijloacelor tehnice speciale, precum şi organelor de control împuternicite în temeiul pct. 5;

j) stabilirea, în mod expres, prin act intern, a subdiviziunii şi a persoanelor antrenate nemijlocit în activitatea licenţiată;

k) reflectarea încadrării personalului în structura organizatorică şi în nomenclatorul de funcţii, aprobate de către conducătorul persoanei juridice. Titularul de licenţă va stabili pentru fiecare specialist condiţiile concrete privind nivelul de studii, de cunoştinţe tehnice şi experienţă de lucru, precum şi atribuţiile

de serviciu, drepturile, responsabilităţile şi cerinţele faţă de regimul de confidenţialitate;

l) asigurarea perfecţionării periodice a persoanelor antrenate nemijlocit în activitatea licenţiată;

m) corespunderea încăperilor destinate pentru proiectarea, producerea sau păstrarea mijloacelor tehnice speciale cu cerinţele privind asigurarea regimului de confidenţialitate;

n) dotarea cu safeuri a încăperilor destinate pentru păstrarea documentaţiei ce ţine de mijloacele tehnice speciale;

o) corespunderea încăperilor deţinute cu normele de igienă, de securitate a muncii şi de protecţie a mediului stabilite de legislaţia în vigoare;

p) dotarea încăperilor deţinute cu sisteme automate de semnalizare pentru situaţii excepţionale şi antiincendiu;

q) deţinerea aparatajului şi utilajului necesare pentru asigurarea procesului tehnologic la proiectarea şi la producerea mijloacelor tehnice speciale, în cazul în care licenţa prevede activitatea respectivă;

r) proiectarea mijloacelor tehnice speciale în conformitate cu sarcina tehnică, coordonată cu beneficiarul (subiect al activităţii speciale de investigaţii);

s) producerea mijloacelor tehnice speciale în bază de contract (acord) încheiat cu organele abilitate să exercite activitate specială de investigaţii, în conformitate cu documentaţia tehnică, cu normativele tehnice şi cu alte documente de reglementare a activităţii în cauză;

t) importul mijloacelor tehnice speciale în bază de contract (acord) încheiat cu organele abilitate să exercite activitatea specială de investigaţii;

u) exportul mijloacelor tehnice speciale pentru organele abilitate să exercite activitatea specială de investigaţii, după coordonarea cu Serviciul de Informaţii şi Securitate. În acest caz, exportul mijloacelor tehnice speciale poate fi efectuat şi prin intermediul titularilor de licenţă din străinătate, la prezentarea documentelor justificative;

v) punerea la dispoziţia beneficiarului a documentaţiei tehnice şi a informaţiei necesare privind utilizarea mijloacelor tehnice speciale;

w) prezentarea semestrială Serviciului de Informaţii şi Securitate a informaţiei statistice privind importul, exportul, proiectarea, producerea şi comercializarea mijloacelor tehnice speciale;

x) prezentarea, la solicitarea Serviciului de Informaţii şi Securitate, a datelor tehnice şi a mostrelor mijloacelor tehnice speciale;

y) asigurarea condiţiilor necesare pentru efectuarea de către autorităţile competente a controlului asupra desfăşurării genului de activitate licenţiat.

Anexa nr. 3

REGULAMENTUL
privind licenţierea activităţii de prestare a serviciilor în domeniul protecţiei criptografice a informaţiei

I. DISPOZIŢII GENERALE

1. Prezentul regulament reglementează activitatea de prestare a serviciilor în domeniul protecţiei criptografice a informaţiei care nu este atribuită la secret de stat.

2. Prestarea serviciilor în domeniul protecţiei criptografice a informaţiei se realizează în baza unui contract scris, semnat de către ambele părţi.

3. În sensul prezentului regulament se definesc următoarele noţiuni:

protecţie criptografică a informaţiei – ansamblu de măsuri orientate spre asigurarea confidenţialităţii şi a integrităţii informaţiei, ce se realizează pe calea transformării criptografice a informaţiei;

mijloace de protecţie criptografică a informaţiei (în continuare – MPCI) – mijloace tehnice şi/sau de program, sisteme şi complexe, care realizează algoritmii de transformare criptografică a informaţiei, destinate protecţiei integrităţii şi confidenţialităţii informaţiei în procesul de prelucrare, păstrare şi transmitere prin canalele de comunicaţii electronice, de asemenea realizează generarea, crearea, distribuirea sau administrarea cheilor criptografice;

mijloace de criptare – mijloace tehnice şi/sau de program, sisteme şi complexe, care realizează algoritmi criptografici, destinate protecţiei informaţiei transmise prin canalele de comunicaţii electronice şi/sau protecţiei informaţiei contra accesului nesancţionat în procesul de prelucrare şi păstrare a informaţiei;

mijloace de protecţie contra impunerii informaţiei false – mijloace tehnice şi/sau de program, sisteme şi complexe, care realizează algoritmi criptografici, destinate pentru protejarea contra impunerii informaţiei false;

transformare criptografică a informaţiei – transformare a informaţiei cu ajutorul unui algoritm criptografic, utilizînd cheile criptografice în scopul protejării informaţiei contra accesului nesancţionat, precum şi al confirmării de către autor a autenticităţii, a integrităţii şi a calităţii informaţiei;

confidenţialitate – proprietate a informaţiei din cadrul sistemului care caracterizează capacitatea acesteia de a nu fi disponibilă sau divulgată persoanelor, entităţilor sau proceselor neautorizate;

criptare – proces de transformare a informaţiei în mesaj cifrat conform regulilor determinate de algoritmul criptografic;

cheie criptografică – element al cifrului ce se foloseşte pentru criptarea/decriptarea unui mesaj dat, pentru aplicarea şi verificarea semnăturii electronice, pentru calcularea codurilor de autenticitate;

integritate – proprietate a informaţiei din cadrul sistemului, care caracterizează veridicitatea, concordanţa şi invariabilitatea acesteia, inclusiv în condiţiile de acţiune intenţionată sau neintenţionată cu scopul modificării sau distrugerii informaţiei respective.

4. MPCI includ:

a) mijloacele de criptare;

b) mijloacele de protecţie contra impunerii informaţiei false;

c) dispozitivele de creare şi/sau de verificare a semnăturii electronice şi a produselor asociate semnăturii electronice;

d) mijloacele de generare a cheilor criptografice.

5. Activitatea de prestare a serviciilor în domeniul protecţiei criptografice a informaţiei include:

a) cifrarea informaţiei prin utilizarea MPCI în interesul persoanelor fizice şi juridice;

b) protecţia informaţiei, în interesul persoanelor fizice şi juridice, prin utilizarea mijloacelor de protejare contra impunerii informaţiei false;

c) punerea la dispoziţia persoanelor fizice şi juridice a reţelelor de comunicaţii protejate prin MPCI, precum şi a mijloacelor de criptare separate;

d) generarea şi distribuirea cheilor criptografice, inclusiv pentru semnătura electronică;

e) montarea, demontarea, implementarea, reglarea, deservirea, reparaţia MPCI;

f) proiectarea sistemelor informaţionale şi de telecomunicaţii, protejate prin MPCI.

6. Prezentul regulament nu se aplică:

a) mijloacelor de protecţie criptografică a informaţiei care sînt componente ale sistemelor de operare şi programelor aplicative, ale căror funcţii criptografice nu pot fi modificate;

b) cardurilor bancare cu microcipuri încorporate, ale căror funcţii criptografice nu pot fi modificate;

c) mijloacelor de protecție criptografică elaborate şi utilizate pentru bancomate, ale căror funcții criptografice nu pot fi modificate;

d) mijloacelor de protecție criptografică a memoriei fiscale, elaborate şi utilizate pentru aparatele de casă;

e) mijloacelor de protecție criptografică care realizează algoritmi criptografici simetrici şi dispun de chei criptografice cu lungimea de pînă la 56 biți inclusiv;

f) mijloacelor de protecție criptografică care realizează algoritmi criptografici asimetrici şi dispun de chei criptografice cu lungimea de pînă la 128 biți inclusiv.

7. Verificarea corespunderii solicitantului de licență şi controlul respectării de către titularul de licență a condițiilor de licențiere pentru activitatea de prestare a serviciilor în domeniul protecției criptografice a informației se efectuează de către Agenția Servicii Publice în comun cu Serviciul de Informații şi Securitate.

II. CONDIȚIILE DE LICENȚIERE A ACTIVITĂȚII DE PRESTARE A SERVICIILOR ÎN DOMENIUL PROTECȚIEI CRIPTOGRAFICE A INFORMAȚIEI

8. În scopul licențierii şi desfăşurării activității de prestare a serviciilor în domeniul protecției criptografice a informației, solicitantul şi titularul de licență trebuie să respecte următoarele condiții:

a) să dețină statut de persoană juridică sau fizică, înregistrată în calitate de întreprinzător;

b) să desfăşoare activitatea licențiată în conformitate cu legislația în vigoare şi standardele în domeniu;

c) să desfăşoare activitatea licențiată în conformitate cu regulile stabilite de organul de licențiere şi autoritatea publică de specialitate;

d) să prezinte, la solicitare, Serviciului de Informații şi Securitate lista MPCI utilizate în activitatea licențiată, documentația tehnică şi/sau mostrele MPCI;

e) să utilizeze MPCI de import doar dacă acestea au fost introduse şi realizate pe teritoriul Republicii Moldova în modul stabilit de legislația în vigoare;

f) să dețină legal, în proprietate sau în posesie, mijloacele tehnice şi/sau de program utilizate în activitatea licențiată;

g) să aplice, în activitatea licențiată, algoritmi criptografici aprobați ca standarde naționale, internaționale sau acceptați de autoritatea publică de specialitate;

h) să dețină legal, în proprietate sau în posesie, spațiile necesare pentru buna desfăşurare a activității licențiate în corespundere cu normele de igienă, de se-

curitate a muncii şi de protecţie a mediului stabilite de legislaţia în vigoare;

i) să asigure regimul de confidenţialitate în activitatea licenţiată, ce prevede nedivulgarea informaţiei privind beneficiarul serviciilor şi conţinutul serviciilor prestate fără consimţămîntul acestuia. Informaţiile respective sînt prezentate doar organelor de drept şi de control, în conformitate cu legislaţia în vigoare;

j) să păstreze în safeuri documentaţia ce vizează MPCI;

k) să elaboreze şi să aprobe, în termen de o lună de la data eliberării licenţei, regulamentul intern în care să fie stabilite condiţiile de organizare a activităţii licenţiate, modul de evidenţă, păstrare, transmitere şi distrugere a MPCI şi a documentaţiei tehnice;

l) să organizeze regimul intern astfel încît să excludă posibilitatea accesului neautorizat la MPCI;

m) să asigure evidenţa strictă a MPCI, documentînd utilizarea, predarea mijloacelor respective beneficiarului, precum şi nimicirea acestora;

n) persoanele care sînt antrenate nemijlocit în activitatea licenţiată trebuie să aibă studii superioare în domeniul protecţiei criptografice a informaţiei fie să aibă studii superioare în alt domeniu şi, concomitent, studii de perfecţionare în domeniul protecţiei criptografice a informaţiei, fie să aibă studii superioare şi vechime în muncă în domeniul protecţiei criptografice a informaţiei de cel puţin 3 ani. Nivelul cunoştinţelor persoanelor respective trebuie să corespundă cerinţelor prevăzute la pct. 9 şi 10 şi se confirmă printr-un certificat privind absolvirea cursurilor specializate în domeniul protecţiei criptografice a informaţiei;

o) să stabilească expres, prin act intern, subdiviziunea şi persoanele antrenate nemijlocit în activitatea licenţiată;

p) să aprobe structura organizatorică, nomenclatorul de funcţii şi fişele de post pentru fiecare specialist;

q) să asigure perfecţionarea periodică a persoanelor antrenate nemijlocit în activitatea licenţiată;

r) să asigure evidenţa şi păstrarea suporturilor cheilor criptografice, să înregistreze eliberarea, restituirea şi nimicirea cheilor criptografice în registre specializate;

s) să asigure păstrarea separată a suporturilor cheilor criptografice şi a suporturilor de rezervă, dacă procesul tehnic şi tehnologic prevede existenţa acestora;

t) să deservească echipamentul utilizat în activitatea licenţiată în conformitate cu reglementările documentaţiei de exploatare;

u) să pună la dispoziţia beneficiarului documentaţia tehnică şi informaţia necesară privind utilizarea MPCI;

v) să asigure condiţiile necesare pentru efectuarea de către autorităţile competente a controlului privind desfăşurarea genului de activitate licenţiat.

9. Persoanele care sînt antrenate nemijlocit în activitatea de prestare a serviciilor în domeniul protecţiei criptografice a informaţiei trebuie să cunoască:

a) prevederile actelor normative în vigoare cu privire la protecţia criptografică a informaţiei;

b) prevederile actelor normative în vigoare cu privire la semnătura electronică;

c) standardele naţionale şi internaţionale (ISO, NIST) în domeniul protecţiei criptografice a informaţiei;

d) standardele naţionale şi internaţionale (ISO, NIST, CWA) în domeniul semnăturii electronice;

e) noţiunile de bază în domeniul protecţiei criptografice a informaţiei, precum transformarea criptografică a informaţiei, generarea, distribuirea şi protecţia cheilor criptografice, contracararea posibilităţilor de compromitere a cheilor criptografice, metodele de generare aleatorie sau pseudoaleatorie de biţi, tehnologiile de protecţie contra impunerii informaţiei false;

f) noţiunile de bază în domeniul semnăturii electronice, precum metodele şi domeniile de aplicare a semnăturii electronice, tehnologiile de creare a semnăturii electronice, contracararea falsificării semnăturii electronice, organizarea infrastructurii cheilor publice;

g) interfeţele de interacţiune dintre sistemul informaţional şi modulul criptografic;

h) limbajele de programare, în scopul realizării algoritmilor criptografici, în cazul prestării serviciilor menţionate la pct. 5 lit. f).

10. Persoanele care sînt antrenate nemijlocit în activitatea de prestare a serviciilor în domeniul protecţiei criptografice a informaţiei trebuie să posede următoarele abilităţi:

a) să pregătească, să planifice şi să organizeze procesul de prestare a serviciilor în domeniul protecţiei criptografice a informaţiei şi a semnăturii electronice;

b) să utilizeze metodele criptografice de protecţie a informaţiei şi a semnăturii electronice;

c) să efectueze analiza sistemelor informaţionale cu module criptografice în scopul evaluării conformităţii nivelului de protecţie a informaţiei;

d) să configureze modulele criptografice pentru asigurarea protecţiei necesare a sistemului informaţional şi pentru asigurarea funcţionalităţii acestuia;

e) să studieze MPCI pentru analiza corectitudinii funcţionării acestora;

f) să înlăture erorile apărute în procesul de exploatare a modulului criptografic.

11. Proprietarul, administratorul şi personalul care este antrenat nemijlocit în activitatea de prestare a serviciilor în domeniul protecţiei criptografice a informaţiei nu trebuie să aibă antecedente penale pentru infracţiuni comise în domeniul tehnologiei informaţiei şi comunicaţiilor electronice.

Anexa nr. 4

REGULAMENTUL
privind licenţierea activităţii de prestare a serviciilor
în domeniul protecţiei tehnice a informaţiei

I. DISPOZIŢII GENERALE

1. Prezentul regulament reglementează activitatea de prestare a serviciilor în domeniul protecţiei tehnice a informaţiei care nu este atribuită la secret de stat.

2. Prestarea serviciilor în domeniul protecţiei tehnice a informaţiei se realizează în baza unui contract scris, semnat de către ambele părţi.

3. Activitatea ce ţine de prestarea serviciilor în domeniul protecţiei tehnice a informaţiei include:

a) efectuarea inspecţiilor tehnice ale încăperilor şi echipamentelor (mijloacelor de prelucrare a informaţiei) cu scopul depistării mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei;

b) instalarea, montarea, reglarea mijloacelor de protecţie tehnică a informaţiei şi mijloacelor tehnice protejate de prelucrare a informaţiei.

4. În sensul prezentului regulament se definesc următoarele noţiuni:

protecţie tehnică a informaţiei – activitate orientată spre descoperirea la timp şi anihilarea ameninţărilor informaţiei, care se realizează prin intermediul metodelor şi mijloacelor tehnice;

cerinţe specifice vizînd protecţia tehnică a informaţiei – act elaborat în baza normelor naţionale şi internaţionale în domeniul protecţiei tehnice a informaţiei, luînd în considerare toate caracteristicile obiectului care trebuie protejat, în care se stabilesc măsurile necesare vizînd protecţia tehnică a informaţiei procesate în sistemele informaţionale şi de comunicaţii electronice sau circulante în încăperile care trebuie protejate;

mijloace tehnice protejate de prelucrare a informaţiei – mijloace tehnice de prelucrare a informaţiei pentru care măsurile necesare de protecţie a informaţiei

procesate sînt realizate la etapa de elaborare şi producere a acestora;

mijloace de protecţie tehnică a informaţiei – mijloace tehnice destinate pentru înlăturarea sau diminuarea posibilităţii de scurgere a informaţiei prin canale tehnice;

mijloace tehnice speciale destinate pentru obţinerea ascunsă a informaţiei – mijloacele tehnice şi/sau de program proiectate, modificate sau programate pentru captarea, obţinerea, interceptarea, culegerea, ascultarea, înregistrarea şi transmiterea semnalelor informaţionale de natură sonoră, vizuală, electromagnetică sau de altă natură, inclusiv din reţelele de comunicaţii electronice, în scopul obţinerii accesului ascuns la informaţia străină. Clasificatorul mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei se aprobă de către Guvern;

mijloace tehnice specializate pentru depistarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei – mijloace tehnice specializate şi mijloace metrologice pentru detectarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei în încăperi şi în echipamente;

inspecţie tehnică – control special al încăperilor şi echipamentelor care se efectuează cu utilizarea mijloacelor tehnice specializate pentru depistarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei.

II. CONDIŢIILE DE LICENŢIERE A ACTIVITĂŢII DE PRESTARE A SERVICIILOR ÎN DOMENIUL PROTECŢIEI TEHNICE A INFORMAŢIEI

5. În scopul licenţierii şi desfăşurării activităţii de prestare a serviciilor în domeniul protecţiei tehnice a informaţiei, solicitantul şi titularul de licenţă trebuie să respecte următoarele condiţii:

a) să deţină statut de persoană juridică sau fizică, înregistrată în calitate de întreprinzător;

b) să desfăşoare activitatea licenţiată în conformitate cu legislaţia în vigoare şi standardele în domeniu;

c) să desfăşoare activitatea licenţiată în conformitate cu regulile stabilite de organul de licenţiere şi autoritatea publică de specialitate;

d) persoanele care sînt antrenate nemijlocit în activitatea licenţiată trebuie să aibă studii superioare în domeniul protecţiei tehnice a informaţiei fie să aibă studii superioare în alt domeniu şi, concomitent, studii de perfecţionare în domeniul protecţiei tehnice a informaţiei, fie să aibă studii superioare şi vechime în muncă în domeniul protecţiei tehnice a informaţiei de cel puţin 3 ani. Nivelul cunoştinţelor persoanelor respective trebuie să corespundă cerinţelor indicate la pct. 6 şi 7;

e) să deţină legal, în proprietate sau în posesie, spaţiile necesare pentru buna desfăşurare a activităţii licenţiate, în corespundere cu normele de igienă, de securitate a muncii şi de protecţie a mediului stabilite de legislaţia în vigoare;

f) în cazul prestării serviciilor indicate la pct. 3 lit. a), să dispună de mijloace tehnice specializate pentru depistarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei, mijloace care sînt specificate la pct. 8;

g) să elaboreze şi să aprobe, în termen de o lună de la data eliberării licenţei, regulamentul intern în care să fie stabilite condiţiile de organizare a activităţii licenţiate;

h) să stabilească expres, prin act intern, subdiviziunea şi persoanele antrenate nemijlocit în activitatea licenţiată;

i) să aprobe structura organizatorică şi nomenclatorul de funcţii. Titularul de licenţă va stabili, prin act intern, pentru fiecare specialist condiţiile concrete privind nivelul de studii, de cunoştinţe tehnice şi experienţă de lucru, precum şi atribuţiile de serviciu, drepturile, responsabilităţile şi cerinţele faţă de regimul de confidenţialitate;

j) să asigure perfecţionarea periodică a persoanelor antrenate nemijlocit în activitatea licenţiată;

k) să elaboreze şi să aprobe, în termen de o lună de la data eliberării licenţei, documentaţia tehnico-normativă vizînd efectuarea nemijlocită a activităţii licenţiate;

l) să asigure regimul de confidenţialitate în activitatea licenţiată, ce prevede nedivulgarea informaţiei vizînd beneficiarul serviciilor şi conţinutul serviciilor prestate, fără consimţămîntul acestuia. Informaţiile respective sînt prezentate doar organelor de drept şi de control, în conformitate cu legislaţia în vigoare;

m) să informeze imediat Serviciul de Informaţii şi Securitate despre cazurile de depistare a mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei;

n) în cazul prestării serviciilor indicate la pct. 3 lit. a), să ţină evidenţa mijloacelor tehnice specializate pentru depistarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei, precum şi evidenţa deservirii tehnice a acestora în conformitate cu cerinţele de exploatare;

o) după prestarea serviciilor, să pună la dispoziţia beneficiarului actul de efectuare a inspecţiei tehnice a încăperilor şi a echipamentelor cu scopul depistării mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei, actul de instalare (montare, reglare) a mijloacelor de protecţie tehnică a informaţiei şi mijloacelor tehnice protejate de prelucrare a informaţiei, perfectate în conformitate cu Regulamentul privind licenţierea activităţii de prestare a serviciilor în domeniul importului, exportului, proiectării, producerii şi comer-

cializării mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informației și cu Regulamentul privind licențierea activității de prestare a serviciilor în domeniul protecției criptografice a informației, precum și în conformitate cu cerințele specifice vizînd protecția tehnică a informațiilor procesate în sistemele informaționale şi de comunicaţii electronice sau circulante în încăperile care trebuie protejate, în funcție de serviciile care au fost prestate;

p) să prezinte, la solicitare, Serviciului de Informații și Securitate datele statistice privind serviciile prestate;

q) să asigure condițiile necesare pentru efectuarea de către autoritățile competente a controlului privind desfăşurarea genului de activitate licențiat.

6. Persoanele care sînt antrenate nemijlocit în activitatea de prestare a serviciilor în domeniul protecției tehnice a informației trebuie să cunoască:

a) prevederile actelor normative în vigoare cu privire la protecția tehnică a informației;

b) noțiunile de bază vizînd originea apariției canalelor tehnice de scurgere a informațiilor procesate în sistemele informaționale şi de comunicaţii electronice sau circulante în încăperi, precum caracteristicile de timp, de frecvență și cele spectrale ale semnalelor analogice şi digitale care circulă în sistemele informaționale şi de comunicaţii electronice sau în încăperi, cauzele de apariție a radiațiilor compromițătoare ale mijloacelor de prelucrare a informațiilor şi a transformărilor acustico-electrice şi celor vibro-acustice ale semnalelor sonore;

c) canalele posibile de scurgere a informațiilor stocate, procesate, transmise prin intermediul sistemelor informaționale și de comunicații electronice sau circulante în încăperi;

d) metodele de anihilare a canalelor posibile de scurgere a informaţiilor procesate în sistemele informaţionale şi de comunicaţii electronice sau circulante în încăperi;

e) principiile de funcţionare a mijloacelor de protecţie tehnică a informaţiei;

f) posibilitățile tehnice ale mijloacelor de protecţie tehnică a informaţiei şi ale mijloacelor tehnice specializate pentru depistarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiilor, ce se află în dotarea acestora;

g) metodele de utilizare a mijloacelor tehnice specializate pentru depistarea mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informațiilor, ce se află în dotarea acestora.

7. Persoanele care sînt antrenate nemijlocit în activitatea de prestare a serviciilor în domeniul protecției tehnice a informației trebuie să posede următoarele abilități:

a) să planifice şi să organizeze inspecţiile tehnice ale încăperilor şi echipamentelor cu scopul depistării mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei şi a analiza rezultatele obţinute;

b) să utilizeze mijloacele tehnice specializate pentru depistarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiilor;

c) să efectueze identificarea, analiza şi evaluarea ameninţărilor privind informaţiile procesate în sistemele informaţionale şi de comunicaţii electronice sau circulante în încăperi şi să elaboreze măsurile adecvate de contracarare a vulnerabilităţilor stabilite;

d) să pregătească documentele necesare cu privire la serviciile prestate

– actul de efectuare a inspecţiei tehnice a încăperilor şi a echipamentelor cu scopul depistării mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei

– cerinţele specifice de protecţie tehnică a informaţiilor procesate în sistemele informaţionale şi de comunicaţii electronice sau circulante în încăperile care trebuie protejate

– actul de instalare (montare, reglare) a mijloacelor de protecţie tehnică a informaţiei şi mijloacelor tehnice protejate de prelucrare a informaţiei.

8. Pentru prestarea serviciilor în domeniul protecţiei tehnice a informaţiei indicate la pct. 3 lit. a), solicitantul de licenţă trebuie să deţină, în mod legal, mijloace tehnice specializate pentru depistarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei, necesare pentru efectuarea inspecţiilor tehnice. Setul minim de echipamente necesare include:

a) detectorul de joncţiuni neliniare pentru detectarea dispozitivelor electronice ascunse;

b) echipamentul pentru detectarea emisiilor radio în banda de frecvenţe 50–2500 MHz;

c) echipamentul pentru analizarea circuitelor fizice (reţele electrice şi cele de tensiune joasă) cu scopul detectării semnalelor în curenţii purtători în banda de frecvenţe 0,05–1MHz.

GUVERNUL

HOTĂRÎRE Nr. 1176 din 22-12-2010

pentru aprobarea Regulamentului cu privire la asigurarea regimului secret n cadrul autorităţilor publice şi al altor persoane juridice

Publicat : 26-08-2011 în Monitorul Oficial Nr. 139-145 art. 686

Versiune în vigoare din 31.10.14 în baza modificărilor prin HG886 din 22.10.14, MO325-332/31.10.14 art.954

În temeiul Legii nr. 245-XVI din 27 noiembrie 2008 cu privire la secretul de stat (Monitorul Oficial al Republicii Moldova, 2009, nr.45-46, art.123), cu modificările ulterioare, Guvernul HOTĂRĂŞTE:

1. Se aprobă Regulamentul cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice (se anexează).

2. În vederea implementării regulamentului nominalizat, autorităţile publice şi alte persoane juridice, care utilizează informaţii atribuite secret de stat, în termen de 3 luni din la data intrării în vigoare a acestuia, vor elabora şi vor aproba normele proprii cu privire la asigurarea regimului secret şi vor întreprinde măsurile necesare pentru realizarea prezentei hotărîri.

3. Cetăţenilor care, la momentul intrării în vigoare a prezentei hotărîri, dispun de dreptul de acces la secretul de stat şi al căror acces a fost coordonat cu Serviciul de Informaţii şi Securitate al Republicii Moldova, li se va menţine acest drept pînă la expirarea termenelor stabilite de art. 24 alin. (2) lit. b) şi alin. (3) din Legea nr. 245-XVI din 27 noiembrie 2008 cu privire la secretul de stat, pentru forma 1 şi, respectiv, forma 2 de acces la secret de stat.

4. Cetăţenii care, la momentul intrării în vigoare a prezentei hotărîri, dispun de dreptul de acces la secret de stat, însă accesul acestora nu a fost coordonat cu Serviciul de Informaţii şi Securitate al Republicii Moldova, vor fi supuşi măsurilor de verificare în termen de 5 ani din data intrării în vigoare a prezentei hotărîri.

5. Autorităţile publice şi alte persoane juridice vor asigura verificarea persoanelor prevăzute în pct.4 din prezenta hotărîre, conform unui plan coordonat cu Serviciul de Informaţii şi Securitate al Republicii Moldova.

6. Se abrogă Hotărîrea Guvernului nr. 638 din 18 septembrie 1995 „Pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în organele puterii legislative, executive, juridice, organele administraţiei publice locale, întreprinderile, instituţiile şi organizaţiile Republicii Moldova”.

REGULAMENT

cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice

Capitolul I

DISPOZIŢII GENERALE PRIVIND ASIGURAREA REGIMULUI SECRET

Secţiunea 1

Consideraţii generale

1. Prezentul Regulament stabileşte modalitatea de asigurare a regimului secret în cadrul autorităţilor publice şi al altor persoane juridice.

2. Regimul secret reprezintă ansamblul de măsuri organizatorico-juridice, care fac parte din sistemul naţional de protecţie a secretului de stat, privind metodele şi mijloacele utilizate de protejare a informaţiilor şi a purtătorilor materiali de informaţii atribuite la secret de stat, precum şi acţiunile întreprinse în acest domeniu, care se referă inclusiv la:

1) secretizarea şi desecretizarea informaţiilor;

2) cerinţele înaintate faţă de autorităţile publice, alte persoane juridice şi personalul acestora cu privire la protecţia secretului de stat;

3) modul de acces la secretul de stat;

4) întocmirea, evidenţa, păstrarea, procesarea, multiplicarea, utilizarea, transmiterea, distrugerea informaţiilor atribuite la secret de stat;

5) protecţia secretului de stat prin măsuri de ordin juridic şi de ordin procedural, măsuri de protecţie fizică, de protecţie a sistemelor informaţionale, de telecomunicaţii, precum şi a personalului;

6) exercitarea controlului asupra măsurilor referitoare la protecţia secretului de stat.

3. În sensul prezentului Regulament se definesc următoarele noţiuni:

autorizaţie de acces la secret de stat – document prin care se confirmă că persoana fizică, titular al acesteia, poate avea acces la secret de stat de un anumit grad de secretizare;

articole secrete – complexele, sistemele şi articolele de înarmare şi tehnică militară, precum şi anumite instalaţii, agregate, blocuri, reţele, dispozitive, materiale, produse chimice, aparataj, utilaj, machete de produse şi altele

asemenea, care fac parte din categoria informaţiilor atribuite la secret de stat;

secretizarea informaţiei – încadrarea informaţiei la un anumit grad de secretizare;

desecretizarea informaţiei – scoaterea informaţiei secretizate de sub incidenţa reglementărilor privind secretul de stat şi suprimarea parafei de secretizare aplicată pe purtătorul material de asemenea informaţie;

certificat de securitate – document prin care se confirmă dreptul persoanelor juridice, cu excepţia autorităţilor publice, de a desfăşura o activitate ce ţine de utilizarea informaţiilor atribuite la secret de stat, crearea mijloacelor de protejare a informaţiei, realizarea măsurilor şi/sau prestarea serviciilor de protecţie a secretului de stat;

zonă de securitate – perimetru delimitat şi special amenajat unde sînt gestionate informaţiile atribuite la secret de stat.

4. Măsurile de protecţie a informaţiilor atribuite la secret de stat trebuie stabilite în raport cu:

1) gradul de secretizare a informaţiilor;

2) volumul şi purtătorii materiali ai informaţiilor;

3) modul de acordare a dreptului de acces la secret de stat;

4) calitatea, funcţia şi numărul persoanelor care au sau pot avea acces la secret de stat;

5) ameninţările, riscurile şi vulnerabilităţile ce pot avea consecinţe asupra informaţiilor atribuite la secret de stat.

Secţiunea a 2-a

Reguli generale privind secretizarea şi desecretizarea informaţiilor

5. Informaţiile din domeniul apărării naţionale, economiei, ştiinţei şi tehnicii, relaţiilor externe, securităţii statului, asigurării ordinii de drept şi activităţii autorităţilor publice sînt secretizate, ţinînd cont de importanţa pe care o au pentru interesele şi/sau securitatea Republicii Moldova şi de consecinţele ce s-ar produce ca urmare a pierderii sau divulgării lor neautorizate.

6. În funcţie de gravitatea prejudiciilor ce pot fi cauzate intereselor şi/sau securităţii Republicii Moldova în cazul divulgării sau pierderii acestor informaţii, Legea nr. 245-XVI din 27 noiembrie 2008 cu privire la secretul de stat (în continuare – Legea) stabileşte 4 grade de secretizare a informaţiilor atribuite la secret de stat şi, respectiv, parafele de secretizare pentru purtătorii materiali de asemenea informaţii:

1) „Strict secret" – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate aduce prejudicii deosebit de grave intereselor şi/sau securităţii

Republicii Moldova;

2) „Secret” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate dăuna grav intereselor şi/sau securităţii Republicii Moldova;

3) „Confidenţial” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate dăuna intereselor şi/sau securităţii Republicii Moldova;

4) „Restricţionat” – grad de secretizare atribuit informaţiilor a căror divulgare neautorizată poate fi în dezavantajul intereselor şi/sau securităţii Republicii Moldova sau poate conduce la divulgarea unei informaţii secretizate cu parafa „Strict secret”, „Secret” sau „Confidenţial”.

7. În corespundere cu gradele de secretizare a informaţiilor atribuite la secret de stat, sînt stabilite următoarele termene de secretizare a informaţiilor, care încep din ziua în care pe purtătorul material de informaţii atribuite la secret de stat a fost aplicată parafa de secretizare:

1) „Strict secret” – pînă la 25 de ani;

2) „Secret” – pînă la 15 ani;

3) „Confidenţial” – pînă la 10 ani;

4) „Restricţionat” – pînă la 5 ani.

8. Termenul de secretizare a informaţiilor despre persoanele care colaborează sau au colaborat confidenţial cu organele ce desfăşoară activitate de informaţii, de contrainformaţii şi operativă de investigaţii este nelimitat, indiferent de gradul de secretizare.

9. Termenul de secretizare a datelor despre identitatea şi calitatea ofiţerului de informaţii este de 50 de ani din data eliberării din serviciu a ofiţerului, dar nu mai puţin de 25 de ani din data decesului acestuia. Termenul poate fi prelungit pe perioade consecutive a cîte 10 ani, la decizia directorului Serviciului de Informaţii şi Securitate, în cazul în care desecretizarea datelor contravine intereselor asigurării securităţii naţionale şi/sau a drepturilor şi intereselor legitime ale urmaşilor ofiţerului de informaţii.

10. Termenele de secretizare pot fi prelungite în anumite situaţii excepţionale de către Comisia interdepartamentală pentru protecţia secretului de stat, în baza unei motivaţii temeinice, la solicitarea conducătorilor autorităţilor publice învestite cu împuterniciri de dispoziţie asupra informaţiilor atribuite la secret de stat sau, după caz, din oficiu.

11. Drept temei pentru secretizarea informaţiilor, elaborate/primite în cadrul activităţii de administrare, de producţie, ştiinţifice şi de altă natură a autorităţilor publice şi altor persoane juridice şi aplicarea parafei de secretizare pe purtătorii lor materiali, este corespunderea cu:

1) prevederile articolelor 7 şi 8 din Lege;

2) Nomenclatorul informaţiilor atribuite la secret de stat;

3) nomenclatoarele departamentale de informaţii care urmează a fi secretizate.

12. Categoriile informaţiilor atribuite la secret de stat se stabilesc conform Nomenclatorului informaţiilor atribuite la secret de stat.

13. În scopul concretizării şi sistematizării informaţiilor în domeniile lor de activitate, autorităţile publice învestite cu împuterniciri de dispoziţie asupra acestor informaţii, elaborează, în baza şi în limitele Nomenclatorului informaţiilor atribuite la secret de stat, nomenclatoare departamentale detaliate de informaţii, care urmează a fi secretizate. După caz, pot fi elaborate şi nomenclatoare interdepartamentale detaliate de informaţii, care urmează a fi secretizate şi care trebuie să corespundă Nomenclatorului informaţiilor atribuite la secret de stat.

14. Pentru elaborarea nomenclatoarelor departamentale detaliate de informaţii care urmează a fi secretizate, în cadrul autorităţilor publice învestite cu împuterniciri de dispoziţie asupra acestora se instituie comisii în componenţa cărora se includ, în mod obligatoriu, şi reprezentanţi ai subdiviziunilor interioare de protecţie a informaţiilor atribuite la secret de stat. În vederea elaborării nomenclatoarelor interdepartamentale detaliate de informaţii care urmează a fi secretizate, se instituie comisii interdepartamentale, în componenţa cărora se includ, în mod obligatoriu, şi reprezentanţi ai subdiviziunilor interioare de protecţie a informaţiilor atribuite la secret de stat din cadrul fiecărei autorităţi publice implicate.

15. În nomenclatorul departamental detaliat de informaţii, care urmează a fi secretizate, trebuie să fie prevăzute categoriile informaţiilor, iar, în caz de necesitate, şi informaţiile aparte privind aspectele de activitate ale autorităţii publice. Gradul de secretizare a acestor informaţii se stabileşte în mod diferenţiat, ţinîndu-se cont de gravitatea prejudiciilor ce pot fi cauzate intereselor şi/sau securităţii Republicii Moldova în cazul divulgării sau pierderii acestor informaţii.

16. Nomenclatoarele departamentale/interdepartamentale detaliate de informaţii, care urmează a fi secretizate, se aprobă de conducătorul autorităţii/ conducătorii autorităţilor publice respective şi conţin informaţii cu împuternicirile de dispoziţie asupra cărora sînt învestite autorităţile publice în cauză, stabilesc gradele şi termenele lor de secretizare.

17. Conţinutul nomenclatoarelor departamentale/interdepartamentale detaliate de informaţii, care urmează a fi secretizate, nu sînt date publicităţii. Ele urmează să fie aduse la cunoştinţa structurilor de subordonare departamentală, precum şi a persoanelor juridice care efectuează lucrări cu utilizarea informaţiilor atribuite la secret de stat, în partea ce se referă la activitatea acestora, pentru a putea fi utilizate la secretizarea informaţiilor. De asemenea, persoanele juridice care efectuează lucrări cu utilizarea informaţiilor atribuite la secret de stat, în

coordonare cu beneficiarul acestor lucrări, pot elabora nomenclatoare detaliate separate de informaţii care urmează a fi secretizate.

18. Secretizarea informaţiei se efectuează prin încadrarea acesteia la un anumit grad de secretizare, potrivit nomenclatorului departamental/ interdepartamental detaliat de informaţii, care urmează a fi secretizate, şi, respectiv, asigurarea aplicării parafei de secretizare, conform gradului de secretizare.

19. Decizia cu privire la secretizarea informaţiei se adoptă de către persoana cu funcţii de răspundere care semnează documentul, la propunerea executantului, şi se manifestă prin aplicarea semnăturii pe suportul material de informaţii.

20. Secretizarea documentelor care se semnează de către conducătorul autorităţii publice sau al altei persoane juridice se efectuează la propunerea şefilor subdiviziunilor interioare care au întocmit documentul.

21. Secretizarea documentelor care se semnează de către şefii subdiviziunilor interioare se efectuează la propunerea executanţilor.

22. Aplicarea parafei de secretizare pe document se asigură de către persoana care-l întocmeşte.

23. Gradul de secretizare a informaţiei se determină în conformitate cu Nomenclatorul informaţiilor atribuite la secret de stat şi nomenclatoarele departamentale/interdepartamentale detaliate de informaţii care urmează a fi secretizate, iar în cazuri aparte – conform părţii care se referă la lucrările ce urmează a fi efectuate în baza acestor nomenclatoare.

24. Gradul de secretizare a informaţiilor ce se conţin în document se determină de executant şi persoana care semnează sau aprobă documentul.

25. Gradul de secretizare a informaţiilor privind efectuarea unor lucrări în comun şi a altor lucrări se determină de către beneficiarul acestor lucrări în comun cu executantul lucrărilor.

26. Gradul de secretizare a informaţiilor ce se conţin în tezele de licenţă, masterat, doctorat, alte lucrări cu tematică secretă, se determină de către executant şi conducătorul lui ştiinţific.

27. Gradul de secretizare a informaţiilor ce se conţin în cererea de înregistrare a dreptului de proprietate intelectuală se determină de către autor (coautori) şi conducătorul autorităţii publice învestite cu împuterniciri de dispoziţie asupra informaţiilor atribuite la secret de stat, care prezintă cererea.

28. Documentul elaborat pe baza prelucrării informaţiilor cu grade de secretizare diferite va fi secretizat conform noului conţinut, care poate fi superior originalelor.

29. Documentul rezultat din cumularea neprelucrată a unor extrase provenite din informaţii secretizate va primi gradul de secretizare corespunzător

conţinutului extrasului cu cel mai înalt nivel de secretizare.

30. Rezumatele, traducerile şi extrasele din documentele secretizate primesc gradul de secretizare corespunzător conţinutului.

31. Dacă unele părţi ale unui document (spre exemplu, pagini, paragrafe, secţiuni, anexe) conţin informaţii ce se atribuie la diferite grade de secretizare, pe acestea se vor aplica parafele corespunzătoare gradului de secretizare respectiv. În acest caz, gradul de secretizare atribuit documentului integral va fi cel al părţii cu cel mai înalt grad de secretizare.

32. Scrisorile sau notele care însoţesc documentele anexate poartă nivelul de secretizare cel mai înalt care a fost atribuit acestora din urmă. Autoritatea emitentă indică în mod clar gradul de secretizare în cazul în care sînt separate de anexele lor.

33. Parafa de secretizare reflectă gradul superior de secretizare a informaţiilor ce se conţin în lucrări, documente, articole şi se marchează prin una din inscripţiile: „Strict secret", „Secret", „Confidenţial" sau „Restricţionat".

34. Parafa de secretizare a lucrării, etapelor şi părţilor ei componente se indică de către beneficiarul acestora în sarcina (planul) de executare a lucrării.

35. Cînd se aplică parafa „Strict secret", se indică, sub linie, punctul din nomenclatorul departamental/interdepartamental detaliat de informaţii care urmează a fi secretizate, în baza căruia se determină parafa.

36. Parafa de secretizare a articolului şi a fiecărei părţi componente a acestuia se indică, de către cel care elaborează sau fabrică, în documentaţia cu privire la articol (spre exemplu, condiţiile tehnice, instrucţiunile privind exploatarea, paşaportul tehnic).

37. Secretizarea informaţiilor care nu corespund criteriilor stabilite în punctul 11 din prezentul Regulament şi, respectiv, aplicarea parafei de secretizare cu privire la aceste informaţii nu se admite.

38. În cazul în care persoanele cu funcţii de răspundere din cadrul autorităţilor publice şi altor persoane juridice consideră că divulgarea anumitor informaţii este de natură să aducă atingere intereselor şi/sau securităţii Republicii Moldova, dar nu pot fi identificate cu cele incluse în nomenclatorul respectiv, vor asigura secretizarea preliminară a acestora, prin aplicarea parafei, conform gradului de secretizare apreciat.

39. Dacă informaţia care nu este prevăzută în nomenclatorul departamental/interdepartamental detaliat de informaţii care urmează a fi secretizate dezvăluie informaţiile ce se conţin în acest nomenclator, atunci acestea trebuie să aibă acelaşi grad de secretizare, care este menţionat în punctele respective ale nomenclatorului.

40. Persoanele responsabile, în termen de o lună de la secretizarea preliminară

a informaţiilor, sînt obligate să prezinte persoanei cu funcţie de răspundere, care a aprobat nomenclatorul respectiv, propuneri de completare/modificare a acestuia, însoţite de o motivaţie temeinică. Pînă la adoptarea unei decizii definitive, caracterul secret al acestor informaţii va fi asigurat în conformitate cu cerinţele prezentului Regulament.

41. După aprecierea informaţiilor secretizate preliminar în conformitate cu prevederile articolului 12 alineatul (3) din Lege, conducătorii autorităţilor publice şi ai altor persoane juridice, care au aprobat nomenclatorul respectiv, vor lua o decizie argumentată, în formă scrisă, cu privire la completarea/modificarea nomenclatorului în vigoare sau scoaterea parafei de secretizare atribuite preliminar.

42. Propunerile de modificare şi/sau completare a Nomenclatorului informaţiilor atribuite la secret de stat, însoţite de motivaţia temeinică, se înaintează Guvernului.

43. Conducătorii autorităţilor publice, învestite cu împuterniciri de dispoziţie asupra informaţiilor atribuite la secret de stat, vor dispune verificarea periodică, dar nu mai rar decît o dată la 5 ani, de regulă, după revizuirea conţinutului nomenclatoarelor departamentale/interdepartamentale detaliate de informaţii care urmează a fi secretizate, a tuturor informaţiilor secrete de stat cărora le-au fost atribuite grade de secretizare, prilej cu care, dacă este necesar, vor fi reevaluate gradele, respectiv, parafele, precum şi termenele de secretizare a acestora. Dacă este posibil, autoritatea emitentă indică pe documentul secretizat data sau termenul începînd cu care informaţiile pe care acesta le cuprinde li se va putea reduce gradul de secretizare sau vor putea fi desecretizate.

44. La finisarea lucrărilor efectuate în comun şi a altor lucrări, integral sau etapizat, beneficiarul acestora în comun cu executantul vor examina chestiunea cu privire la păstrarea sau modificarea gradului de secretizare a informaţiilor stabilit anterior şi, în caz de necesitate, vor opera modificări şi completări la capitolul respectiv al sarcinii în vederea executării lucrărilor.

45. Modificarea gradului de secretizare a informaţiilor implică, în mod obligatoriu, modificarea parafei de secretizare pe purtătorii materiali şi/sau în documentaţia de însoţire a acestora.

46. Modificarea parafei de secretizare se efectuează în conformitate cu prevederile articolului 15 din Lege.

47. În termen de 6 luni de la data stabilită de reducere a gradului de secretizare categoriilor de informaţii prevăzute în Nomenclatorul informaţiilor atribuite la secret de stat şi în nomenclatoarele departamentale de informaţii care urmează a fi secretizate, autorităţile publice sau alte persoane juridice, în temeiul deciziei conducătorilor autorităţilor publice cu împuterniciri de dispoziţie asupra acestor informaţii, vor asigura modificarea parafei de secretizare a purtătorilor materiali de informaţii atribuite la secret de stat.

48. În toate celelalte cazuri, modificarea parafei de secretizare a purtătorilor materiali de informaţii atribuite la secret de stat se efectuează, în temeiul deciziei persoanei cu funcţie de răspundere care a secretizat informaţia sau a succesorului ei de drept, în termen de 3 luni de la data stabilită de reducere a gradului de secretizare a informaţiilor conţinute de ele.

49. Modificarea parafei de secretizare în cazul majorării gradului de secretizare a informaţiilor se face imediat, în temeiul deciziei scrise a persoanei cu funcţie de răspundere care a secretizat informaţia sau a succesorului ei de drept.

50. Decizia cu privire la modificarea parafei de secretizare urmează să fie argumentată şi se emite în formă scrisă.

51. Persoana cu funcţii de răspundere care a secretizat informaţia sau succesorul ei de drept, în cel mai restrîns termen, informează despre decizia cu privire la modificarea parafei de secretizare autorităţile sau persoanele juridice cărora le-a fost expediat documentul, iar acestea, la rîndul lor, au responsabilitatea de a informa destinatarii succesivi cărora le-au transmis originalul documentului sau o copie a acestuia. În baza deciziei menţionate, autorităţile sau persoanele juridice destinatare efectuează modificarea respectivă a parafei de secretizare a documentului.

52. În cazul în care propunerea cu privire la secretizarea sau modificarea parafei de secretizare a fost înaintată de către autoritatea publică sau persoana juridică care a primit documentul, expeditorul va informa destinatarul documentului despre decizia luată, indiferent de caracterul acesteia.

53. Privitor la modificarea parafei de secretizare a documentelor şi articolelor se efectuează înscrieri în registrele de evidenţă respective, în fişe, pe documente, în documentaţia tehnică (de însoţire) a articolelor. Data şi noul grad de secretizare vor fi indicate pe document deasupra sau sub vechea inscripţie, care va fi anulată prin trasarea unei linii oblice.

54. Informaţiile secrete de stat se desecretizează de către persoanele cu funcţii de răspundere cu împuterniciri de secretizare a informaţiilor respective dacă:

1) termenul de secretizare a expirat;

2) s-au schimbat circumstanţele obiective şi, drept urmare, protecţia în continuare a anumitor informaţii atribuite la secret de stat devine inoportună;

3) au fost operate modificări în articolele 7 şi 8 din Lege, în Nomenclatorul informaţiilor atribuite la secret de stat sau în nomenclatoarele departamentale/ interdepartamentale detaliate de informaţii care urmează a fi secretizate şi, drept urmare, protecţia în continuare a anumitor informaţii atribuite la secret de stat devine inoportună;

4) există o decizie privind recunoaşterea secretizării informaţiilor drept neîntemeiată.

55. Persoanele cu funcţii de răspundere care au emis documente secrete vor evalua periodic necesitatea de desecretizare sau de micşorare a gradului de secretizare acordat anterior acestora. Ori de cîte ori este posibil, emitentul unui document secretizat trebuie să precizeze dacă acesta poate fi desecretizat ori trecut la un grad inferior de secretizare, la o anumită dată sau la producerea unui anumit eveniment.

56. În scopul evaluării necesităţii de desecretizare sau de micşorare a gradului de secretizare acordat informaţiilor, pot fi create comisii speciale în componenţa cărora va fi inclusă, în mod obligatoriu, o persoană din cadrul Subdiviziunii de protecţie a informaţiilor atribuite la secret de stat, care dispune de forma de acces corespunzătoare gradului de secretizare a acestor informaţii.

57. Decizia cu privire la desecretizarea informaţiilor se adoptă de către persoanele cu funcţii de răspundere cu împuterniciri de secretizare a informaţiilor respective. Această decizie se emite în formă scrisă şi urmează să fie argumentată.

58. Comisia interdepartamentală pentru protecţia secretului de stat, precum şi conducătorii autorităţilor publice şi ai altor persoane juridice sînt împuterniciţi de a desecretiza informaţiile care au fost secretizate neîntemeiat de către persoanele cu funcţii de răspundere din subordine.

59. În cazul păstrării informaţiilor atribuite la secret de stat în fondurile închise ale arhivelor, purtătorii materiali ai acestora se vor desecretiza de către conducătorii arhivelor de stat, cu condiţia că organizaţia întemeietoare a fondului sau succesorul ei de drepturi le deleagă astfel de împuterniciri. În caz de lichidare a organizaţiei întemeietoare a fondului şi de lipsă a succesorului ei de drepturi, chestiunea privind desecretizarea purtătorilor materiali de informaţii atribuite la secret de stat este examinată de Comisia interdepartamentală pentru protecţia secretului de stat.

60. Persoanele cu funcţii de răspundere împuternicite de a secretiza informaţiile vor asigura informarea autorităţilor sau persoanelor juridice, cărora le-a fost expediat documentul, despre faptul desecretizării acestuia.

61. Informaţiile secretizate, despre care s-a stabilit cu certitudine că sînt divulgate sau iremediabil pierdute, vor fi desecretizate. Desecretizarea se face numai în baza investigaţiei prin care s-a stabilit faptul divulgării sau pierderii informaţiilor respective ori a suportului material al acestora, cu acordul scris al emitentului.

62. În cazul în care se consideră că anumite informaţii au fost secretizate neîntemeiat, cetăţenii sau persoanele juridice sînt în drept să conteste decizia de secretizare, în conformitate cu prevederile articolului 17 din Lege.

Secţiunea a 3-a

Subdiviziunile interioare de protecţie a informaţiilor atribuite la secret de stat

63. În scopul implementării acţiunilor cu privire la asigurarea regimului secret şi organizarea controlului permanent privind respectarea măsurilor de protecţie a informaţiilor atribuite la secret de stat în autorităţile publice şi alte persoane juridice trebuie să existe, în condiţiile Legii, subdiviziuni interioare de protecţie a informaţiilor atribuite la secret de stat (în continuare – Subdiviziuni de protecţie), cu atribuţii specifice.

64. Crearea, reorganizarea şi lichidarea Subdiviziunilor de protecţie se efectuează în baza deciziei (ordinului) conducătorilor autorităţilor publice sau altor persoane juridice deţinătoare de informaţii atribuite la secret de stat, prin coordonare cu Serviciul de Informaţii şi Securitate. La crearea noilor Subdiviziuni de protecţie, Serviciul de Informaţii şi Securitate verifică existenţa condiţiilor necesare pentru funcţionarea normală a acestora.

65. Funcţiile, drepturile, obligaţiile, organizarea Subdiviziunii de protecţie se stabilesc în regulamentul de funcţionare al acesteia, elaborat în conformitate cu cerinţele prezentului Regulament, coordonat cu Serviciul de Informaţii şi Securitate şi aprobat de conducătorul autorităţii publice sau al altor persoane juridice.

66. În funcţie de volumul şi importanţa activităţilor ce implică informaţii atribuite la secret de stat, Subdiviziunile de protecţie pot include subdiviziuni de regim secret, care organizează asigurarea şi respectarea regimului secret în autorităţile publice sau alte persoane juridice, şi subdiviziuni ale lucrărilor de secretariat secrete, care elaborează şi înfăptuiesc măsuri ce ţin de asigurarea regimului secret la executarea lucrărilor de secretariat secrete cu efectuarea controlului asupra respectării lor. De asemenea, reieşind din specificul activităţii şi volumul informaţiilor atribuite la secret de stat în cadrul autorităţilor publice sau al altor persoane juridice, pot fi create grupuri de lucru, secţii sau unităţi secrete, iar în cadrul acestora pot fi numiţi reprezentanţi ai Subdiviziunii de protecţie.

67. În autorităţile publice sau alte persoane juridice unde se efectuează un volum mare de lucrări secrete pot fi numiţi locţiitori ai conducătorilor autorităţilor publice sau persoanelor juridice, responsabili de asigurarea regimului secret.

68. Atunci cînd autorităţile publice sau alte persoane juridice efectuează un volum redus de lucrări cu informaţii atribuite la secret de stat, acţiunile cu privire la asigurarea regimului secret şi organizarea controlului permanent privind respectarea măsurilor de protecţie a informaţiilor atribuite la secret de stat se realizează de către conducătorul acestora sau de către o persoană numită prin ordin special de către conducător. În acest caz, atribuţiile Subdiviziunii de protecţie vor fi îndeplinite de persoana respectivă.

69. Subdiviziunea de protecţie coordonează activitatea altor subdiviziuni în partea ce ţine de asigurarea protecţiei secretului de stat şi se subordonează nemijlocit conducătorului autorităţii publice sau al altei persoane juridice şi locţiitorului responsabil de asigurarea regimului secret.

70. Se interzice angajarea temporară a persoanelor în Subdiviziunea de protecţie, în subdiviziunile de cifrare sau mobilizare ale autorităţilor publice sau ale altor persoane juridice.

71. Desemnarea persoanelor în funcţia de locţiitori ai conducătorilor autorităţilor publice şi ai altor persoane juridice, responsabili de asigurarea regimului secret, a şefilor Subdiviziunilor de protecţie, precum şi eliberarea acestora din funcţie se efectuează prin coordonare cu Serviciul de Informaţii şi Securitate.

72. În cadrul Subdiviziunilor de protecţie sînt angajate persoanele care au drept de acces la secret de stat, dau dovadă de cunoştinţe necesare şi au experienţă în organizarea regimului secret.

73. Şeful Subdiviziunii de protecţie trebuie să dispună de dreptul de acces la secret de stat, corespunzător celui mai înalt grad de secretizare a informaţiilor gestionate de autoritatea publică sau altă persoană juridică respectivă.

74. La desemnarea în/eliberarea din funcţie a persoanelor din cadrul Subdiviziunii de protecţie se va efectua inventarierea documentelor şi altor purtători materiali de informaţii atribuite la secret de stat, aflate în gestiunea persoanelor respective, prin întocmirea unui proces-verbal de predare-primire.

75. Pentru efectuarea inventarierii poate fi instituită, după caz, o comisie formată din cel puţin trei persoane, care dispun de forma de acces la secret de stat corespunzătoare celui mai înalt grad de secretizare a informaţiilor care urmează a fi predate-primite.

76. În timpul inventarierii se verifică existenţa documentelor şi a altor purtători materiali de informaţii atribuite la secret de stat, prin confruntarea cu datele indicate în actele de evidenţă.

77. În autorităţile publice şi alte persoane juridice unde se efectuează controale anuale privind verificarea disponibilului documentelor şi altor purtători materiali de informaţii atribuite la secret de stat, cu perfectarea actelor corespunzătoare, în procesul-verbal de predare-primire se permite a se indica numărul documentelor şi altor purtători materiali de informaţii atribuite la secret de stat pentru fiecare an în parte, iar pentru perioada care a expirat de la ultimul control anual se indică numărul documentelor şi altor purtători materiali de informaţii atribuite la secret de stat transmise şi primite, în conformitate cu toate tipurile de evidenţă. Cînd lipsesc actele controlului anual pe o anumită perioadă, în procesul-verbal de primire-predare se reflectă pentru fiecare an în parte numărul documentelor şi altor purtători materiali de informaţii atribuite

la secret de stat luate în evidenţă şi a celor existente, în conformitate cu toate tipurile de evidenţă.

78. În procesul-verbal de predare-primire se indică, de asemenea, încălcările de regim depistate, alte date cu privire la starea de lucruri a Subdiviziunii de protecţie. Eventualele obiecţii şi explicaţii se anexează la procesul-verbal de predare-primire.

79. Despre constatarea lipsei unor documente sau altor purtători materiali de informaţii atribuite la secret de stat se informează neîntîrziat conducătorul autorităţii sau al altei persoane juridice, iar acesta din urmă va informa, după caz, Subdiviziunea de protecţie a instituţiei ierarhic superioare şi/sau Serviciul de Informaţii şi Securitate.

80. Procesul-verbal trebuie să fie semnat de persoana care predă documentele şi alţi purtători materiali de informaţii atribuite la secret de stat, persoana care le primeşte, după caz, membrii comisiei de predare-primire, şi va fi aprobat de conducătorul autorităţii publice sau al altei persoane juridice.

81. În cazul absenţei temporare a şefului Subdiviziunii de protecţie (concediu, delegare, caz de boală), se întocmeşte un proces-verbal de predare-primire a documentelor şi altor purtători materiali de informaţii atribuite la secret de stat necesare în lucru. Procesul-verbal se semnează de către şeful Subdiviziunii de protecţie, după caz, conducătorul autorităţii publice sau al altei persoane juridice şi persoana numită pentru îndeplinirea obligaţiilor acestuia, care dispune de forma corespunzătoare de acces la secret de stat. Persoana numită pentru îndeplinirea obligaţiilor şefului Subdiviziunii de protecţie nu poartă răspundere pentru documentele şi alţi purtători materiali de informaţii atribuite la secret de stat care se păstrează în safeuri, dulapuri de metal, depozite, alţi suporţi speciali, dacă integritatea amprentelor ştampilelor pe acestea este păstrată.

82. Subdiviziunea de protecţie are următoarele sarcini de bază:

1) preîntîmpinarea accesului neîntemeiat la informaţiile atribuite la secret de stat;

2) descoperirea şi lichidarea surselor de divulgare a informaţiilor atribuite la secret de stat în procesul de activitate a autorităţilor publice şi altor persoane juridice;

3) asigurarea regimului secret în procesul efectuării tuturor lucrărilor secrete de către autorităţile publice şi alte persoane juridice;

4) organizarea lucrărilor de secretariat secrete.

83. Subdiviziunea de protecţie are următoarele atribuţii generale:

1) elaborează şi propune spre aprobare conducerii autorităţii publice sau a altei persoane juridice actele normative interne cu privire la protecţia informaţiilor atribuite la secret de stat, monitorizează aplicarea normelor în vigoare de

protecţie a secretului de stat;

2) participă la elaborarea nomenclatoarelor departamentale/interdepartamentale detaliate de informaţii care urmează a fi secretizate şi a altor acte normative ce reglementează modul departamental de asigurare a regimului secret;

3) elaborează, în comun cu şefii subdiviziunilor interioare, Nomenclatorul funcţiilor care necesită acces la secretul de stat;

4) coordonează activitatea de protecţie a informaţiilor atribuite la secret de stat şi efectuează controlul asupra îndeplinirii cerinţelor în vigoare cu privire la asigurarea regimului secret, inclusiv în procesul lucrărilor de secretariat, analizează aspectele activităţii autorităţii publice sau al altei persoane juridice în vederea preîntîmpinării, depistării şi lichidării încălcării normelor de protecţie a secretului de stat;

5) întocmeşte Programul de prevenire a scurgerii de informaţii atribuite la secret de stat şi îl supune avizării Serviciului de Informaţii şi Securitate, iar după aprobare, acţionează pentru aplicarea acestuia;

6) informează Serviciul de Informaţii şi Securitate despre cazurile de divulgare a informaţiilor secrete, precum şi despre dispariţia documentelor şi altor purtători materiali de informaţii secrete;

7) participă din oficiu la efectuarea investigaţiilor privind faptele de încălcare a regimului secret;

8) asigură colaborarea cu alte instituţii referitor la protecţia secretului de stat;

9) consiliază conducerea autorităţii publice sau a altei persoane juridice în legătură cu toate aspectele ce ţin de protecţia secretului de stat;

10) informează conducerea autorităţii publice sau al altei persoane juridice despre vulnerabilităţile şi riscurile existente în sistemul de protecţie a informaţiilor atribuite la secret de stat şi propune măsuri pentru înlăturarea acestora;

11) acordă sprijin Serviciului de Informaţii şi Securitate privind verificarea cetăţenilor care necesită perfectarea (reperfectarea) dreptului de acces la secret de stat;

12) organizează activităţi de instruire specifică a personalului autorităţilor publice sau altor persoane juridice care au acces la secret de stat;

13) ţine evidenţa persoanelor pentru care a fost perfectat (reperfectat) dreptul de acces la secret de stat, asigură păstrarea autorizaţiilor de acces şi a certificatului de securitate eliberat persoanei juridice;

14) ţine evidenţa safeurilor, dulapurilor de metal, depozitelor speciale şi altor încăperi în care se permite păstrarea documentelor şi altor purtători materiali de informaţii secrete;

15) exercită alte atribuţii în domeniul protecţiei secretului de stat, potrivit Legii şi prezentului Regulament.

84. Atribuţiile personalului din Subdiviziunea de protecţie se stabilesc prin fişa postului, aprobată de conducătorul autorităţii publice sau al altei persoane juridice. Se interzice implicarea personalului din Subdiviziunea de protecţie în executarea altor obligaţii ce nu decurg din prevederile prezentului Regulament.

85. Pregătirea profesională a angajaţilor Subdiviziunilor de protecţie în domeniul asigurării regimului secret se asigură de către autorităţile publice sau persoanele juridice respective.

Capitolul II

DREPTUL DE ACCES LA SECRETUL DE STAT

Secţiunea 1

Accesul cetăţenilor la secretul de stat

86. Accesul la secretul de stat este permis cu respectarea principiului necesităţii de a lucra cu informaţii atribuite la secret de stat numai cetăţenilor care deţin autorizaţie de acces la secretul de stat, valabilă pentru gradul de secretizare a informaţiilor necesare activităţii efectuate.

87. Accesul cetăţenilor la secretul de stat se perfectează (reperfectează) benevol în condiţiile stabilite de Lege şi prezentul Regulament şi este permis cetăţenilor Republicii Moldova cu capacitate deplină de exerciţiu, începînd cu vîrsta de 18 ani, care:

1) şi-au exprimat în scris consimţămîntul pentru aplicarea măsurilor de verificare din partea organelor competente;

2) au fost supuşi măsurilor de verificare în legătură cu perfectarea dreptului de acces la secretul de stat;

3) şi-au asumat în scris obligaţia privind păstrarea secretului de stat care le va fi încredinţat;

4) şi-au exprimat în scris acordul pentru limitarea drepturilor lor în legătură cu accesul la secretul de stat;

5) au fost familiarizaţi, contra semnătură, cu normele ce prevăd răspunderea pentru încălcarea legislaţiei privind secretul de stat.

88. Dreptul de acces la secretul de stat se acordă prin ordin sau dispoziţie scrisă:

1) de către conducătorul autorităţii publice sau al altei persoane juridice în care persoana lucrează, îşi îndeplineşte serviciul sau studiază;

2) de către persoana cu funcţii de răspundere care numeşte în funcţie conducătorul autorităţii publice sau al altei persoane juridice;

3) de către conducătorul autorităţii publice sau al altei persoane juridice care este beneficiară a lucrărilor legate de secretul de stat, în cazul în care autoritatea publică sau persoana juridică nu este subordonată altei autorităţi publice sau al altei persoane juridice ori nu intră în domeniul lor de administrare;

4) de către conducătorul autorităţii publice sau al altei persoane juridice unde se desfăşoară activitatea legată de secretul de stat, dacă solicitarea persoanei de a dispune de informaţii atribuite la secret de stat nu este legată de locul său de muncă, de serviciu sau de studii.

89. La perfectarea dreptului de acces la secretul de stat se va decide asupra compensaţiei care urmează a fi acordată persoanei în legătură cu îndeplinirea permanentă a lucrărilor ce prevăd accesul la secretul de stat, în mărimea şi modul stabilit de Guvern.

90. Modul de acces la secretul de stat pentru Preşedintele Republicii Moldova, Preşedintele Parlamentului şi deputaţii în Parlament, Prim-ministru, membrii Guvernului, preşedintele Curţii Constituţionale, preşedintele Curţii Supreme de Justiţie, Procurorul General, directorul Serviciului de Informaţii şi Securitate, directorul Serviciului de Protecţie şi Pază de Stat, guvernatorul Băncii Naţionale a Moldovei, preşedintele Curţii de Conturi, Avocatul Poporului şi adjuncţii Avocatului Poporului, preşedintele Comisiei Naţionale a Pieţei Financiare, preşedinţii de raioane şi conducătorii altor autorităţi administrative centrale prevăzute de Legea nr.64-XII din 31 mai 1990 cu privire la Guvern este reglementat de articolul 28 alineatul (1) din Lege.

(se completează prin HG886 din 22.10.14, MO325-332/31.10.14 art.954)

91. Accesul cetăţenilor străini şi al apatrizilor la secretul de stat se acordă în cazuri excepţionale, în condiţiile stabilite de articolul 28 alineatul (4) din Lege.

92. În funcţie de gradul de secretizare a informaţiilor, sînt stabilite următoarele forme de acces la secretul de stat:

1) forma 1 – pentru lucrul cu informaţii atribuite la secret de stat avînd gradele de secretizare „Strict secret", „Secret", „Confidenţial" şi „Restricţionat";

2) forma 2 – pentru lucrul cu informaţii atribuite la secret de stat avînd gradele de secretizare „Secret", „Confidenţial" şi „Restricţionat";

3) forma 3 – pentru lucrul cu informaţii atribuite la secret de stat avînd gradul de secretizare „Confidenţial" şi „Restricţionat";

4) forma 4 – pentru lucrul cu informaţii atribuite la secret de stat avînd gradul de secretizare „Restricţionat".

93. Dreptul de acces la secretul de stat se perfectează pentru următoarele

termene:

1) forma 1 – 5 ani;

2) forma 2 – 7 ani;

3) forma 3 – 9 ani;

4) forma 4 – 12 ani.

94. Durata dreptului de acces la secretul de stat nu poate depăşi durata atribuţiilor care au servit drept temei pentru acordarea acestuia.

95. Numărul persoanelor cărora urmează să li se perfecteze dreptul de acces la informaţiile atribuite la secret de stat trebuie să fie strict determinat în funcţie de necesitatea utilizării unor astfel de informaţii în procesul activităţii desfăşurate şi se va stabili în Nomenclatorul funcţiilor care necesită acces la secretul de stat (în continuare – Nomenclatorul funcţiilor), aprobat de către conducătorul autorităţii publice sau al altei persoane juridice (forma nr. 1, anexă la prezentul Regulament) şi avizat de către Serviciul de Informaţii şi Securitate. Orice modificare/completare ce se operează în Nomenclatorul funcţiilor se avizează de către Serviciul de Informaţii şi Securitate.

96. Nomenclatorul funcţiilor se reexaminează cel puţin o dată la 5 ani pentru a verifica dacă funcţiile aprobate corespund formei de acces indicate şi principiului necesităţii de a lucra cu informaţii atribuite la secret de stat. Dacă se va constata că Nomenclatorul funcţiilor nu mai corespunde cerinţelor existente, se va întocmi unul nou. La prezentarea acestuia spre avizare Serviciului de Informaţii şi Securitate, autoritatea publică sau altă persoană juridică va indica în scrisoarea de însoţire cînd a fost avizat precedentul Nomenclator al funcţiilor, numărul de persoane şi forma de acces prevăzută pentru funcţiile respective. Dacă numărul funcţiilor/persoanelor din Nomenclator se majorează, se va indica motivul majorării.

97. Materialele referitoare la cetăţenii care necesită perfectarea (reperfectarea) dreptului de acces la secretul de stat se pregătesc de către subdiviziunea resurse umane, iar acolo unde aceasta lipseşte – de către persoana responsabilă de lucrul cu personalul.

98. În scopul perfectării dreptului de acces la secretul de stat, cetăţenii Republicii Moldova completează Chestionarul de bază (forma nr. 2, anexă la prezentul Regulament) şi prezintă 2 fotografii color de mărimea 4,5 x 6 cm. Pentru perfectarea dreptului de acces la informaţiile cu gradul de secretizare „Strict secret” şi „Secret”, concomitent cu Chestionarul de bază se completează un Chestionar suplimentar (forma nr. 3, anexă la prezentul Regulament). Toate datele indicate de către cetăţean trebuie să fie autentice.

99. Cetăţenii care necesită perfectarea dreptului de acces la secretul de stat îşi manifestă în prealabil acordul scris cu privire la aplicarea măsurilor de

verificare din partea organelor competente.

100. Subdiviziunea resurse umane sau persoana responsabilă de lucrul cu personalul în procesul pregătirii materialelor referitoare la cetăţenii care necesită perfectarea dreptului de acces la secretul de stat confruntă informaţia indicată în Chestionarul de bază (suplimentar) cu datele din actele corespunzătoare (buletin de identitate, livret militar, alte acte), concretizează dacă cetăţeanul a avut anterior acces la secretul de stat, care formă de acces i-a fost perfectată, alte aspecte necesare perfectării dreptului de acces.

101. Orice modificare ulterioară a datelor indicate în Chestionarul de bază (suplimentar) se va comunica neîntîrziat subdiviziunii resurse umane sau persoanei responsabile de lucrul cu personalul.

102. Subdiviziunea resurse umane sau persoana responsabilă de lucrul cu personalul vizează şi prezintă Subdiviziunii de protecţie materialele referitoare la perfectarea dreptului de acces la secretul de stat.

103. Subdiviziunea de protecţie din cadrul autorităţii publice sau al altei persoane juridice care perfectează dreptul de acces la secretul de stat verifică prezenţa sau lipsa circumstanţelor prevăzute în articolul 25 alineatul (1) literele a), d), e) şi h) din Lege. În acest sens, pot fi solicitate actele confirmative necesare.

104. Pentru aplicarea măsurilor de verificare, autoritatea publică sau altă persoană juridică va înainta Serviciului de Informaţii şi Securitate o solicitare motivată (forma nr. 5, anexă la prezentul Regulament), în scopul iniţierii măsurilor de verificare privind existenţa sau lipsa circumstanţelor prevăzute în articolul 25 alineatul (1) literele b), c), f), g), i), j) şi k) din Lege. Solicitarea va fi însoţită de Chestionarul de bază, după caz, Chestionarul suplimentar şi Lista rudelor şi persoanelor apropiate, întocmit potrivit modelului din forma nr. 6, anexă la prezentul Regulament, care include: tata, mama, fraţii, surorile, copiii care au împlinit vîrsta de 16 ani, soţia (soţul), fosta soţie (fostul soţ), concubinul (concubina), cumnaţii (cumnatele), ce se completează şi se introduc în plic separat şi sigilat. La prima poziţie din Lista rudelor şi persoanelor apropiate, se indică angajatul supus măsurilor de verificare.

105. Procedura de verificare în vederea acordării accesului la secretul de stat are drept scop identificarea riscurilor de securitate, aferente gestionării informaţiilor secrete de stat.

106. Măsurile de verificare urmează a fi efectuate de către Serviciul de Informaţii şi Securitate în termen de o lună de la data primirii solicitării autorităţii publice sau al altei persoane juridice, numărul acestora fiind direct proporţional gradului de secretizare a informaţiilor la care va avea acces persoana.

107. Ori de cîte ori apar indicii că titularul autorizaţiei de acces la secretul de stat nu mai îndeplineşte criteriile de compatibilitate privind accesul la

informaţiile atribuite la secret de stat, măsurile de verificare se reiau la solicitarea conducătorului autorităţii publice sau al altei persoane juridice.

108. În baza rezultatelor măsurilor de verificare, Serviciul de Informaţii şi Securitate formulează concluzia cu privire la posibilitatea sau imposibilitatea de a acorda cetăţeanului dreptul de acces la secretul de stat (forma nr. 7, anexă la prezentul Regulament), care se perfectează în 2 exemplare, unul dintre care se remite solicitantului, iar celălalt se păstrează la Serviciul de Informaţii şi Securitate.

109. Concluzia cu privire la imposibilitatea de acordare cetăţeanului a dreptului de acces la secretul de stat trebuie să conţină temeiul corespunzător prevăzut în articolul 25 alineatul (1) din Lege, care a servit drept bază pentru adoptarea ei. Aceasta este executorie pentru persoanele cu funcţii de răspundere împuternicite să adopte decizia privind acordarea dreptului de acces la secretul de stat, însă nu exclude posibilitatea înaintării unei solicitări repetate după înlăturarea circumstanţelor care fac imposibilă acordarea dreptului de acces la secretul de stat.

110. În termen de 5 zile de la primirea concluziei Serviciului de Informaţii şi Securitate, conducătorul autorităţii publice sau al altei persoane juridice va adopta decizia cu privire la acordarea dreptului de acces la secretul de stat şi va elibera autorizaţia de acces de forma corespunzătoare (forma nr. 8, anexă la prezentul Regulament) sau va refuza acordarea dreptului de acces la secretul de stat.

111. Imediat după primirea concluziei pozitive a Serviciului de Informaţii şi Securitate şi pînă la adoptarea deciziei cu privire la acordarea dreptului de acces la secretul de stat, cetăţeanul este familiarizat, contra semnătură, de către Subdiviziunea de protecţie cu dispoziţiile legale privind protecţia secretului de stat şi limitarea unor drepturi ale acestuia în legătură cu accesul la secretul de stat, precum şi cu normele ce prevăd răspunderea pentru încălcarea legislaţiei cu privire la secretul de stat şi semnează angajamentul de confidenţialitate (forma nr. 4, anexă la prezentul Regulament).

112. În decizia cu privire la acordarea dreptului de acces la secretul de stat se va indica: forma de acces la secretul de stat, termenul pentru care se perfectează, numele, prenumele, funcţia cetăţeanului căruia, se acordă dreptul de acces la secretul de stat, cuantumul compensaţiei stabilite în legătură cu îndeplinirea lucrărilor ce prevăd accesul la secretul de stat.

113. Decizia privind refuzul de acordare a dreptului de acces la secretul de stat se adoptă în temeiul prevederilor articolului 25 din Lege, se comunică în scris solicitantului şi poate fi atacată în organul ierarhic superior sau în instanţa de judecată.

114. Pentru confirmarea dreptului de acces la secretul de stat în raport cu terţii, Subdiviziunea de protecţie eliberează cetăţeanului, în temeiul dispoziţiei

conducătorului autorităţii publice sau al altei persoane juridice, un certificat de acces la secretul de stat de forma corespunzătoare (forma nr. 9, anexă la prezentul Regulament), în care se indică activitatea (delegaţie, însărcinare) ce implică accesul la informaţii secretizate, pe care acesta urmează să o îndeplinească. Certificatul se restituie Subdiviziunii de protecţie imediat ce a fost îndeplinită activitatea pentru care a fost eliberat. Evidenţa certificatelor respective se asigură potrivit Registrului de evidenţă a certificatelor de acces la secretul de stat (forma nr.10, anexă la prezentul Regulament).

115. Şeful Subdiviziunii de protecţie va asigura evidenţa strictă a tuturor cetăţenilor cărora le-a fost perfectat dreptul de acces la secretul de stat şi a autorizaţiilor de acces eliberate în Registrul de evidenţă privind accesul la secret de stat (forma nr. 11, anexă la prezentul Regulament). În cazul în care, potrivit legislaţiei în vigoare, datele despre identitatea şi calitatea cetăţenilor nu pot fi divulgate, evidenţa acestora se va ţine într-un registru separat.

116. Despre eliberarea autorizaţiei de acces la secretul de stat va fi informat Serviciul de Informaţii şi Securitate (forma nr. 12, anexă la prezentul Regulament). La scrisoarea de informare se va anexa Fişa de evidenţă a persoanei care dispune de acces la secret de stat (forma nr. 13, anexă la prezentul Regulament).

117. În cazuri excepţionale, determinate de situaţii de criză, calamităţi sau evenimente imprevizibile, conducătorul autorităţii publice sau al altei persoane juridice poate acorda acces temporar la informaţiile atribuite la secret de stat anumitor cetăţeni care nu deţin autorizaţie de acces, cu condiţia asigurării unui sistem corespunzător de evidenţă.

118. Cetăţenii care primesc dreptul de acces temporar la informaţiile atribuite la secret de stat vor semna angajamentul de confidenţialitate, iar informaţia despre aceştia va fi comunicată Serviciului de Informaţii şi Securitate, în cel mai scurt timp posibil, pentru efectuarea măsurilor de verificare, conform procedurii stabilite.

119. În cazul informaţiilor „Strict secrete" şi „Secrete", accesul temporar va fi acordat, pe cît posibil, cetăţenilor care au deja acces la informaţiile atribuite la un anumit grad de secretizare.

120. Pentru personalul Serviciului de Informaţii şi Securitate, procedura de verificare, perfectare (reperfectare) a dreptului de acces la secret de stat şi de evidenţă a autorizaţiilor de acces se reglementează prin acte normative interne.

121. Cetăţenii care au acces la secretul de stat vor respecta cu stricteţe obligaţiile privind păstrarea secretului de stat, stabilite în articolul 29 din Lege. Ei vor fi instruiţi, obligatoriu, cu privire la protecţia informaţiilor atribuite la secret de stat, înaintea începerii activităţii, iar ulterior, la intervale prestabilite şi ori de cîte ori este nevoie.

122. Instruirea personalului se realizează de către Subdiviziunea de

protecţie şi urmăreşte însuşirea corectă a cerinţelor de securitate şi a modului de implementare eficientă a măsurilor de protecţie a informaţiilor atribuite la secret de stat.

123. Activitatea de instruire se efectuează planificat, în scopul prevenirii, contracarării şi eliminării riscurilor şi ameninţărilor la adresa securităţii informaţiilor atribuite la secret de stat.

124. Instruirea personalului se realizează diferenţiat, potrivit gradului de secretizare a informaţiilor la care autorizaţia de acces permite accesul şi va fi înscrisă de către Subdiviziunea de protecţie în Fişa individuală de instruire (forma nr. 14, anexă la prezentul Regulament).

125. După fiecare instruire, cetăţeanul care deţine autorizaţie de acces va semna că a luat act de conţinutul reglementărilor privind protecţia informaţiilor atribuite la secret de stat.

126. Organizarea şi coordonarea activităţii de instruire a Subdiviziunilor de protecţie se va asigura de către Serviciul de Informaţii şi Securitate.

127. Reperfectarea dreptului de acces la secretul de stat se efectuează cu respectarea condiţiilor necesare perfectării dreptului de acces la secretul de stat, în cazurile:

1) expirării termenului pentru care a fost perfectat acest drept, dacă este necesar să se lucreze în continuare cu informaţii atribuite la secret de stat;

2) perfectării unei alte forme de acces la secret de stat în legătură cu necesitatea de a lucra cu informaţii atribuite la secret de stat cu un grad mai înalt de secretizare.

128. Pentru reperfectarea dreptului de acces la secretul de stat, măsurile de verificare se raportează la perioada scursă de la eliberarea autorizaţiei de acces anterioare.

129. Dacă există necesitatea să se lucreze în continuare cu informaţii atribuite la secret de stat de acelaşi grad de secretizare, eliberarea unei noi autorizaţii de acces la secretul de stat nu se efectuează la reperfectarea dreptului de acces în legătură cu expirarea termenului pentru care a fost perfectat acest drept. În acest caz, pe autorizaţia de acces la secretul de stat anterioară se va aplica menţiunea privind prelungirea termenului de valabilitate, cu indicarea termenului nou.

130. Menţiunea privind prelungirea termenului de valabilitate poate fi aplicată pe autorizaţia de acces la secretul de stat pînă la expirarea termenului anterior de valabilitate al acesteia. În această situaţie, termenul nou de valabilitate al autorizaţiei de acces va începe din ultima zi calendaristică în care a expirat termenul anterior de valabilitate al ei.

131. Dreptul de acces la secretul de stat se suspendă sau încetează în conformitate cu prevederile articolului 27 din Lege, la decizia persoanei cu

funcţii de răspundere împuternicită să adopte decizia cu privire la acordarea acestui drept.

132. Termenul pentru care a fost suspendat dreptul de acces la secretul de stat nu prelungeşte termenul de valabilitate al autorizaţiei de acces la secretul de stat.

133. În cazul în care se constată existenţa temeiurilor de încetare a dreptului de acces la secretul de stat, autorizaţia de acces îşi încetează valabilitatea şi se distruge în baza unui proces-verbal.

134. Faptul suspendării, încetării valabilităţii, distrugerii autorizaţiei de acces se consemnează în Registrul de evidenţă privind accesul la secretul de stat.

135. Prelungirea termenului de valabilitate, suspendarea sau încetarea valabilităţii autorizaţiei de acces la secretul de stat se comunică Serviciului de Informaţii şi Securitate, în modul stabilit în forma nr. 12, anexă la prezentul Regulament.

Secţiunea a 2-a

Accesul persoanelor juridice la secretul de stat

136. Dreptul de acces la secretul de stat se acordă persoanelor juridice, cu excepţia autorităţilor publice care desfăşoară activităţi ce ţin de utilizarea informaţiilor atribuite la secret de stat, crearea mijloacelor de protejare a informaţiei, realizarea măsurilor şi/sau prestarea serviciilor de protecţie a secretului de stat, în baza certificatului de securitate eliberat de Comisia interdepartamentală pentru protecţia secretului de stat (în continuare – Comisia interdepartamentală), în modul stabilit de Lege şi prezentul Regulament.

137. Comisia interdepartamentală eliberează certificatul de securitate doar după efectuarea unei expertize speciale a persoanei juridice privind existenţa condiţiilor pentru desfăşurarea activităţii legate de secretul de stat şi atestării conducătorului acesteia. La eliberarea certificatului de securitate, persoanele juridice trebuie să posede un Program de prevenire a scurgerii de informaţii atribuite la secret de stat, avizat conform reglementărilor în vigoare.

138. Pentru obţinerea certificatului de securitate, persoanele juridice depun la Comisia interdepartamentală o cerere (forma nr. 15, anexă la prezentul Regulament), la care anexează formularul completat al Chestionarului de securitate (forma nr. 16, anexă la prezentul Regulament), introdus într-un plic separat şi sigilat şi Programul de prevenire a scurgerii de informaţii atribuite la secret de stat. Documentele ce confirmă datele indicate în chestionarul de securitate se prezintă în copii legalizate notarial. În caz contrar, copiile vor fi confirmate prin prezentarea originalului.

139. Comisia interdepartamentală va asigura înregistrarea corespunzătoare a tuturor documentelor prezentate de către solicitant pentru obţinerea certificatului

de securitate.

140. În termen de 5 zile de la primirea cererii, Comisia interdepartamentală va remite formularul completat al chestionarului de securitate şi o copie a Programului de prevenire a scurgerii de informaţii atribuite la secret de stat Serviciului de Informaţii şi Securitate, solicitînd efectuarea expertizei speciale a persoanei juridice privind existenţa condiţiilor pentru desfăşurarea activităţii legate de secretul de stat.

141. Expertiza specială se efectuează în termen de pînă la 2 luni din momentul solicitării şi are ca obiectiv verificarea:

1) îndeplinirii cerinţelor stabilite de articolul 32 alineatul (3) din Lege, în volumul necesar pentru asigurarea protecţiei informaţiilor utilizate la efectuarea lucrărilor, corespunzător gradului de secretizare a acestora;

2) autenticităţii şi/sau caracterului complet al datelor prezentate de către solicitant.

142. În vederea desfăşurării măsurilor de expertizare, persoana juridică are obligaţia să permită accesul reprezentanţilor Serviciului de Informaţii şi Securitate în sedii, la echipamente, la activităţi, respectiv, să prezinte documentele necesare şi să furnizeze, la cerere, alte date şi informaţii.

143. Ori de cîte ori apar indicii că titularul certificatului de securitate nu mai îndeplineşte condiţiile necesare pentru desfăşurarea activităţii legate de secretul de stat, măsurile de expertizare se reiau.

144. În baza rezultatelor măsurilor de expertizare, Serviciul de Informaţii şi Securitate formulează concluzia cu privire la îndeplinirea sau neîndeplinirea condiţiilor pentru desfăşurarea activităţii legate de secretul de stat (forma nr. 17, anexă la prezentul Regulament). Concluzia se întocmeşte în 2 exemplare, dintre care unul se păstrează la Serviciul de Informaţii şi Securitate, iar altul se remite Comisiei interdepartamentale.

145. Concluzia cu privire la neîndeplinirea condiţiilor pentru desfăşurarea activităţii legate de secretul de stat trebuie să conţină temeiul corespunzător expus în articolul 32 alineatul (3) din Lege şi/sau în punctul 141 din prezentul Regulament, care a servit drept bază pentru adoptarea acesteia. Concluzia nu exclude posibilitatea efectuării unei expertize repetate după înlăturarea circumstanţelor care nu corespund cerinţelor necesare pentru desfăşurarea activităţii legate de secretul de stat.

146. În vederea eliberării certificatului de securitate, Comisia interdepartamentală, în termen de cel mult 5 zile de la primirea concluziei cu privire la existenţa condiţiilor pentru desfăşurarea activităţii legate de secretul de stat, va organiza şi va efectua atestarea conducătorului persoanei juridice.

147. Atestarea constă în aprecierea cunoştinţelor conducătorului persoanei

juridice în domeniul secretului de stat. Aprecierea se efectuează în baza unui interviu de atestare în cadrul căruia conducătorul persoanei juridice este chestionat cu privire la reglementările în vigoare în domeniul secretului de stat.

148. Şedinţa Comisiei interdepartamentale ce ţine de atestarea conducătorului persoanei juridice se consideră deliberativă dacă la ea sînt prezenţi 2/3 din numărul total de membri. Decizia Comisiei interdepartamentale se ia prin vot deschis, cu simpla majoritate de voturi a membrilor Comisiei.

149. Rezultatele atestării se reflectă în Fişa de atestare (forma nr. 18, anexă la prezentul Regulament), care se întocmeşte de către secretarul Comisiei interdepartamentale, se semnează de membrii acesteia şi se aduce la cunoştinţa conducătorului persoanei juridice supus atestării, contra semnătură.

150. În termen de 5 zile de la primirea încheierii de expertiză de la Serviciul de Informaţii şi Securitate sau, după caz, de la atestarea conducătorului persoanei juridice, Comisia interdepartamentală eliberează persoanei juridice Certificatul de securitate (forma nr. 19, anexă la prezentul Regulament) sau refuză eliberarea acestuia.

151. Pentru fiecare gen de activitate, care face obiectul certificatului de securitate, Comisia stabileşte condiţiile pe care trebuie să le respecte solicitantul.

152. În decizia cu privire la refuzul de eliberare a certificatului de securitate trebuie să fie indicat temeiul respectiv.

153. Eliberarea certificatului de securitate este refuzată în cazul:

1) neîndeplinirii cerinţelor stabilite de articolul 32 alineatul (3) din Lege, în volumul necesar pentru asigurarea protecţiei informaţiilor utilizate la efectuarea lucrărilor, corespunzător gradului de secretizare a acestora;

2) prezentării unor date neautentice şi/sau incomplete de către solicitant.

154. Evidenţa certificatelor de securitate eliberate se realizează de către Comisia interdepartamentală, conform Registrului de evidenţă a certificatelor de securitate (forma nr. 20, anexă la prezentul Regulament).

155. Certificatul de securitate eliberat trebuie să conţină:

1) denumirea organului care l-a eliberat;

2) seria, numărul şi data eliberării. Seria se formează din ultimele două cifre ale anului în care se eliberează certificatul de securitate, iar numărul corespunde numărului de ordine din Registrul de evidenţă a certificatelor de securitate;

3) gradul de secretizare a informaţiilor la care se permite accesul;

4) denumirea completă a persoanei juridice;

5) sediul persoanei juridice;

6) numărul de identificare de stat;

7) genul (genurile) de activitate pentru care se acordă accesul;

8) condiţiile stabilite pentru practicarea genului (genurilor) de activitate;

9) termenul de valabilitate al certificatului de securitate;

10) după caz, date cu privire la prelungirea, suspendarea termenului de valabilitate al certificatului de securitate; date cu privire la modificarea denumirii, sediului persoanei juridice; date cu privire la folosirea serviciilor prestate de către Subdiviziunea de protecţie a altei persoane juridice;

11) semnătura preşedintelui Comisiei interdepartamentale, amprenta ştampilei.

156. Termenul de valabilitate al certificatului de securitate este determinat de perioada de desfăşurare a activităţii legate de secretul de stat, dar nu mai mult de un an.

157. Se interzice transmiterea certificatului de securitate de la o persoană juridică la alta, precum şi utilizarea unui singur certificat de securitate de către mai multe persoane juridice.

158. În cazul în care genul de activitate autorizat prin certificatul de securitate se practică în mai multe obiecte (unităţi) separate teritorial (spre exemplu, filiale, reprezentanţe), solicitantului, odată cu certificatul, i se eliberează copii legalizate ale acestuia cu indicarea adresei fiecărui obiect.

159. Copiile certificatelor de securitate urmează a fi înregistrate în Registrul de evidenţă a certificatelor de securitate.

160. În cazul în care după eliberarea certificatului de securitate intervin modificări în datele prezentate de către solicitant la eliberarea certificatului, acesta este obligat, în termen de pînă la 15 zile, să comunice aceste modificări Comisiei interdepartamentale. Concomitent, solicitantul va prezenta Comisiei documentele care confirmă modificările intervenite, certificatul de securitate eliberat, după caz, copiile acestuia, în vederea operării modificărilor de rigoare.

161. Comisia interdepartamentală, în termen de 15 zile, va introduce modificările necesare în certificatul de securitate.

162. Pînă la restituirea certificatului de securitate solicitantului (inclusiv pînă la eliberarea noilor copii de pe acesta), persoana juridică va activa în baza unei copii legalizate, eliberate de Comisia interdepartamentală pentru această perioadă. La eliberarea certificatului de securitate cu modificările de rigoare, solicitantul va restitui Comisiei interdepartamentale copia legalizată.

163. Distrugerea certificatului de securitate se interzice, cu excepţia cazurilor prevăzute în punctul 173 din prezentul Regulament. Nu se admite pierderea certificatului de securitate. În caz că a intervenit una dintre situaţiile menţionate, solicitantul comunică acest fapt Comisiei interdepartamentale într-un termen cît

mai restrîns, însă nu mai tîrziu de 3 zile. Pentru termenul de valabilitate rămas al certificatului de securitate se eliberează un duplicat.

164. Dacă există necesitatea de a continua activitatea legată de secretul de stat după expirarea termenului de valabilitate al certificatului de securitate, persoana juridică va solicita prelungirea valabilităţii acestuia pe termenul prevăzut în punctul 156 din prezentul Regulament.

165. Cererea cu privire la prelungirea termenului de valabilitate al certificatului de securitate se depune la Comisia interdepartamentală cu cel puţin 3 luni înainte de expirarea termenului anterior de valabilitate al certificatului de securitate. La cerere se anexează documentele care confirmă necesitatea prelungirii termenului de valabilitate al certificatului.

166. Prelungirea termenului de valabilitate al certificatului de securitate se efectuează cu respectarea condiţiilor necesare eliberării acestuia.

167. Pe certificatul de securitate se va aplica menţiunea privind prelungirea termenului de valabilitate, cu indicarea termenului nou. Menţiunea privind prelungirea termenului de valabilitate poate fi aplicată pe certificatul de securitate pînă la expirarea termenului anterior de valabilitate al acestuia. În acest caz, termenul nou de valabilitate al certificatului de securitate va începe din ultima zi calendaristică în care a expirat termenul anterior de valabilitate al acestuia.

168. Dreptul de acces la secret de stat al persoanelor juridice este suspendat în cazurile în care:

1) împotriva acesteia a fost pornită urmărirea penală pentru săvîrşirea unei infracţiuni incompatibile cu activitatea ce presupune utilizarea informaţiilor atribuite la secret de stat, pînă la pronunţarea hotărîrii judecătoreşti definitive şi irevocabile;

2) este necesară efectuarea unei expertize suplimentare în legătură cu posibila apariţie a circumstanţelor care nu corespund condiţiilor prevăzute în punctul 141 din prezentul Regulament, pînă la terminarea măsurilor de expertiză, dar nu mai mult de 30 de zile;

3) suspendarea activităţii persoanei juridice, pe un termen ce nu va depăşi termenul de valabilitate al certificatului de securitate.

169. Decizia cu privire la suspendarea dreptului de acces la secretul de stat al persoanei juridice se comunică acesteia în termen de 10 zile din data emiterii.

170. Pe perioada suspendării, certificatul de securitate, după caz, copiile legalizate de pe acesta şi duplicatul se retrag de către Comisia interdepartamentală. La expirarea termenului de suspendare, certificatul de securitate se restituie persoanei juridice sau se distruge în baza unui proces-verbal.

171. Dreptul de acces la secretul de stat al persoanelor juridice încetează în

cazurile:

1) apariţiei sau descoperirii circumstanţelor care nu corespund cerinţelor stabilite în articolul 32 alineatul (3) din Lege;

2) depistării unor date neautentice şi/sau incomplete la eliberarea certificatului de securitate;

3) expirării termenului pentru care a fost perfectat, dacă nu a fost solicitată prelungirea acestuia;

4) suspendării activităţii persoanei juridice pe un termen ce depăşeşte termenul de valabilitate al certificatului de securitate;

5) încălcării, chiar şi o singură dată, a obligaţiilor asumate ce ţin de protecţia secretului de stat;

6) dizolvării persoanei juridice.

172. Decizia cu privire la încetarea dreptului de acces la secretul de stat al persoanei juridice se comunică acesteia în termen de 10 zile din data emiterii.

173. La încetarea dreptului de acces la secretul de stat al persoanei juridice, certificatul de securitate se retrage de către Comisia interdepartamentală şi se distruge în baza unui proces-verbal.

174. Faptul suspendării, încetării, distrugerii certificatului de securitate se consemnează în Registrul de evidenţă a certificatelor de securitate.

Capitolul III

REGULI DE GESTIONARE A PURTĂTORILOR MATERIALI DE INFORMAŢII ATRIBUITE LA SECRET DE STAT

Secţiunea 1

Cerinţe generale cu privire la purtătorii materiali de informaţii atribuite la secret de stat

175. Orice tip de purtători materiali de informaţii atribuite la secret de stat trebuie să fie identificat printr-un anumit număr de componente, amplasate conform cerinţelor prezentului Regulament.

176. Documentele şi alţi purtători materiali de informaţii atribuite la secret de stat trebuie să conţină:

1) parafa de secretizare;

2) numărul de înregistrare;

3) data de înregistrare şi termenul de secretizare a informaţiilor;

4) funcţia, numele, prenumele şi semnătura persoanei cu funcţie de răspundere care a secretizat informaţiile.

177. Pe toate documentele ce conţin informaţii atribuite la secret de stat se aplică în mod obligatoriu parafa de secretizare. Parafa de secretizare se aplică pe toate exemplarele documentului, în partea dreaptă superioară a fiecărei file.

178. Atunci cînd documentul urmează să fie distribuit în mai multe exemplare, fiecare dintre acestea va purta numărul de exemplare, care apare pe prima pagină, sub parafa de secretizare, împreună cu numărul total de file.

179. Pe documentele care sînt adresate unei anumite persoane se aplică suplimentar, sub parafa de secretizare, menţiunea „Personal", iar cele ce se referă la mobilizare, se marchează cu litera „M".

180. Fiecărui document i se atribuie un număr de înregistrare care se înscrie pe toate exemplarele documentului şi pe anexele acestora. Numărul de înregistrare este urmat de menţiunile: „SS" – pentru informaţiile avînd gradul de secretizare „Strict secret, „S" – pentru informaţiile avînd gradul de secretizare „Secret", „C" – pentru informaţiile avînd gradul de secretizare „Confidenţial" şi „R" – pentru informaţiile avînd gradul de secretizare „Restricţionat".

181. La înscrierea numărului de înregistrare se va indica în mod obligatoriu data.

182. Termenul de secretizare a informaţiilor începe de la data la care pe document a fost aplicată parafa de secretizare.

183. Fiecare filă a documentului trebuie să fie numerotată, avînd înscris numărul curent al paginii, urmat de numărul total al acestora. Filele fiecărei anexe la document vor fi numerotate separat.

184. La sfîrşitul documentului se indică funcţia, numele, prenumele persoanei cu funcţie de răspundere care a secretizat informaţiile, cu aplicarea semnăturii acesteia, precum şi numele, prenumele, semnătura celui care a întocmit documentul.

185. Cînd documentele ce conţin informaţii atribuite la secret de stat se semnează de o singură persoană, datele privind funcţia, numele şi prenumele acesteia se înscriu sub text, în centrul paginii.

186. Dacă documentele se semnează de două sau mai multe persoane, funcţia, numele şi prenumele conducătorului autorităţii publice sau al altei persoane juridice se înscriu în partea stîngă, iar ale celorlalţi semnatari – în partea dreaptă, în ordinea corespunzătoare funcţiilor.

187. Cînd documentele care conţin informaţii atribuite la secret de stat se emit în comun de două sau mai multe autorităţi publice sau alte persoane juridice, denumirile acestora se înscriu separat în antet, iar la sfîrşit se semnează de către conducătorii autorităţilor publice sau persoanelor juridice respective,

de la stînga la dreapta, aplicîndu-se ştampilele corespunzătoare.

188. Pe documente se menţionează, după caz, destinatarul. Pentru documentul care urmează să fie expediat la cinci şi mai mulţi destinatari se întocmeşte o listă de expediere, aprobată de către persoana cu funcţie de răspundere care a secretizat şi a semnat documentul. În acest caz, pe fiecare exemplar se indică un singur destinatar. Lista de expediere se coordonează cu Subdiviziunea de protecţie.

189. Documentul destinat unei alte autorităţi publice sau al altei persoane juridice se va întocmi pe foaie cu antet.

190. Exemplarul documentului de ieşire, care rămîne în dosar, poate să nu fie întocmit pe foaie cu antet, însă acesta trebuie să conţină celelalte elemente necesare, inclusiv numărul de înregistrare, data şi menţiunea cu privire la funcţia, numele, prenumele persoanei cu funcţie de răspundere care a secretizat şi a semnat documentul, confirmată prin semnătura executantului.

191. În situaţia în care documentul de bază este însoţit de anexe, la sfîrşitul textului se indică, pentru fiecare anexă: numărul anexei, denumirea (dacă denumirea anexei este indicată în textul documentului, atunci în anexă denumirea nu se indică), numărul de înregistrare, numărul de file al acesteia şi gradul de secretizare. La expedierea documentelor prin scrisoare de însoţire, se va indica suplimentar numărul de exemplare anexate şi numărul total de file.

192. În cazurile în care există un număr mare de anexe, se poate face inventarierea lor cu indicarea elementelor necesare ale documentelor incluse în anexă, iar în scrisoarea de însoţire se scrie: „Anexă conform inventarului nr. _____ pe _____ file”.

193. Anexele se secretizează în funcţie de conţinutul lor, şi nu de cel al documentelor pe care le însoţesc.

194. Scrisoarea de însoţire a documentului nu va cuprinde informaţii detaliate referitoare la conţinutul documentelor anexate.

195. Documentele anexate se semnează, dacă este cazul, de persoanele care au semnat documentul iniţial.

196. Întocmirea documentelor ce conţin informaţii atribuite la secret se stat, respectiv, multiplicarea acestora, se face într-un număr strict limitat de exemplare.

197. Informaţiile atribuite la secret de stat vor fi marcate, inscripţionate şi gestionate numai de către persoanele care au autorizaţie de acces la secretul de stat de forma corespunzătoare.

198. Parafa de secretizare se aplică prin ştampilare, dactilografiere, tipărire sau olograf.

199. Porţiunile clar identificabile din documentele complexe secretizate, cum sînt secţiunile, capitolele, titlurile, anexele, paragrafele, alte părţi componente, care au grade diferite de secretizare sau care nu sînt secretizate, trebuie marcate corespunzător gradului de secretizare.

200. Parafa de secretizare va fi aplicată separat de celelalte menţiuni, cu caractere şi/sau culori diferite.

201. Toate documentele secretizate aflate în lucru sau în stadiu de proiect vor avea înscrisă menţiunea „Proiect" şi vor fi marcate potrivit gradului de secretizare a informaţiilor ce le conţin. Gestionarea documentelor secretizate, aflate în lucru sau în stadiu de proiect, se face în aceleaşi condiţii ca şi ale celor în formă definitivă.

202. Atunci cînd se utilizează documente secretizate pentru întocmirea unui alt document, menţiunile de pe documentele secretizate le vor determina pe cele ale documentului rezultat. Pe documentul rezultat se vor preciza, după caz, documentele sursă care au stat la baza întocmirii lui.

203. Numărul şi data iniţială de înregistrare a documentului secretizat trebuie păstrate, chiar dacă i se aduc amendamente, pînă cînd documentul respectiv va face obiectul revizuirii gradului de secretizare.

204. În cazul în care menţiunile nu pot fi aplicate nemijlocit pe purtătorul material de informaţii atribuite la secret de stat, ele se indică în documentaţia de însoţire a acestuia.

205. Fotografiile, filmele, microfilmele şi negativele lor, rolele, bobinele, containerele sau alţi suporţi de păstrare a acestora se marchează vizibil cu o etichetă care indică parafa de secretizare, numărul şi data înregistrării.

206. Microfilmele trebuie să aibă afişat, la cele două capete, parafa de secretizare, iar la începutul rolei – lista elementelor de conţinut.

207. Gradul de secretizare a informaţiilor înregistrate pe benzi audio se imprimă verbal, atît la începutul înregistrării, cît şi la sfîrşitul acesteia.

208. Marcarea gradului de secretizare pe benzi video trebuie să asigure afişarea pe ecran a parafei de secretizare. În cazul în care, înainte de înregistrarea benzilor, nu se poate stabili cu exactitate gradul de secretizare, parafa se aplică prin inserarea unui segment de bandă la începutul şi la sfîrşitul benzii video.

209. Benzile audio şi video care conţin informaţii atribuite la secret de stat păstrează gradul de secretizare cel mai înalt atribuit pînă în momentul:

1) distrugerii printr-un procedeu autorizat;

2) atribuirii unui grad mai înalt de secretizare prin adăugarea unei înregistrări cu grad superior de secretizare.

210. Proiecţiile de imagini trebuie să afişeze, la începutul şi la sfîrşitul

acestora, numărul şi data înregistrării, precum şi parafa de secretizare.

211. Rolele, bobinele, containerele sau alţi suporţi de păstrare a benzilor magnetice, inclusiv cele video, pe care au fost imprimate informaţii atribuite la secret de stat, vor avea înscris, la loc vizibil, cea mai înaltă parafă de secretizare atribuită acestora, care va rămîne aplicată pînă la distrugerea sau demagnetizarea lor.

212. La efectuarea unei înregistrări pe bandă magnetică, atît la începutul, cît şi la sfîrşitul fiecărui pasaj, se va menţiona gradul de secretizare. În cazul detaşării de pe suportul fizic, fiecare capăt al benzii va fi marcat, la loc vizibil, cu parafa de secretizare.

213. În toate cazurile, ambalajele sau suporţii în care se păstrează documente sau materiale ce conţin informaţii atribuite la secret de stat vor avea marcată parafa de secretizare, numărul şi data înregistrării şi li se va ataşa o listă cu denumirea acestora.

Secţiunea a 2-a

Evidenţa şi circulaţia documentelor secrete

214. Conducătorii autorităţilor publice sau altor persoane juridice vor asigura măsurile necesare de evidenţă şi control a informaţiilor secretizate, astfel încît să se poată stabili, în orice moment, locul în care se află aceste informaţii.

215. Lucrările de secretariat secrete în cadrul autorităţilor publice sau altor persoane juridice se organizează şi se efectuează de către Subdiviziunile de protecţie (subdiviziunile lucrărilor de secretariat secrete).

216. În cadrul Subdiviziunilor de protecţie trebuie să fie create condiţiile necesare pentru lucrul cu informaţii atribuite la secret de stat, conform cerinţelor prezentului Regulament.

217. Evidenţa documentelor (de intrare, de ieşire, interne) şi a altor purtători materiali de informaţii atribuite la secret de stat se ţine, conform registrelor de evidenţă, în formă manuală şi/sau electronică.

218. Ţinerea manuală a registrelor poate fi efectuată sub formă de fişier sau prin introducerea menţiunilor în cartea pentru înregistrări.

219. Drept principiu de bază al evidenţei se consideră atribuirea fiecărui document de intrare şi de ieşire a unui singur număr de înregistrare. La evidenţa pe fişe, pentru fiecare document se întocmeşte o singură fişă de evidenţă, într-un număr necesar de exemplare.

220. În autorităţile publice sau alte persoane juridice unde există un număr neînsemnat de documente de intrare, de ieşire şi interne (pînă la 500 pe an), se permite evidenţa lor conform Registrului de evidenţă a documentelor de intrare, de ieşire şi a celor interne (forma nr.21, anexă la prezentul Regulament), cu un număr unic de ordine.

221. Toate registrele (cărţile pentru înregistrări şi fişele de evidenţă) se înregistrează în Registrul unic de evidenţă a registrelor şi dosarelor finalizate, conform modelului din forma nr. 22, anexă la prezentul Regulament, în care se înregistrează din momentul deschiderii, avînd un număr propriu de evidenţă.

222. Cărţile pentru înregistrări trebuie să fie şnuruite, iar filele numerotate şi sigilate cu ştampila Subdiviziunii de protecţie. Numărul de file se indică pe ultima pagină şi se autentifică de către şeful Subdiviziunii de protecţie, prin aplicarea semnelor de control: semnătura şi ştampila.

223. La finele anului, numărul de fişe din fişierul finisat se indică în registrul unic de evidenţă al registrelor, dosarelor finalizate. Înscrierea finală, autentificată de către şeful Subdiviziunii de protecţie, cu indicarea numărului total de fişe, se face pe o filă aparte, plasată la începutul sau sfîrşitul fişierului.

224. Înregistrarea în registrul manual trebuie executată astfel încît să excludă posibilitatea de a fi radiată (ştearsă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ştergerii, distrugerii). Rectificările, modificările şi completările registrului se autentifică prin semnătura persoanei din cadrul Subdiviziunii de protecţie, cu indicarea datei.

225. Gradul de secretizare a registrelor de evidenţă se determină în funcţie de gradul de secretizare a informaţiilor ce se conţin în ele.

226. Evidenţa documentelor avînd gradul de secretizare „Strict secret" se ţine separat.

227. În registre se reflectă datele cu privire la circulaţia documentelor, din momentul primirii sau întocmirii pînă la finisarea executării şi clasarea lor în dosare, transmiterea destinatarului sau distrugerea lor.

228. Pentru asigurarea controlului şi executarea documentelor se ţine Registrul de evidenţă şi control (forma nr. 23, anexă la prezentul Regulament) sau se vor întocmi fişiere informative.

229. Rezoluţia referitoare la document se face pe o fişă ataşabilă (fişă de însoţire), care se păstrează împreună cu documentul şi prevede executantul, indicaţia nemijlocită, termenul de execuţie, semnătura conducătorului autorităţii publice sau altei persoane juridice şi data. Responsabil pentru executarea documentului este persoana al cărei nume este indicat primul în rezoluţie, dacă nu a fost numită o altă persoană.

230. La înscrierea rezoluţiilor, efectuarea însemnărilor pe documente, precum şi la fiecare recipisă de primire şi restituire a documentelor se indică în mod obligatoriu data.

231. Răspunsul din partea unei subdiviziuni la un document poate fi dat sub formă de rezoluţie sau referinţă sumară direct pe fişa ataşabilă (fişă de însoţire) la documentul respectiv, care se restituie expeditorului împreună cu

documentul, conform numărului de intrare. Concomitent în registrul de evidenţă a documentelor de intrare se indică numărul şi data expedierii. În acelaşi mod se permite a expedia spre executare instituţiilor subordonate interpelările parvenite de la alte autorităţi publice sau persoane juridice.

232. Documentele semnate de către conducătorii autorităţilor publice sau ai altor persoane juridice, care urmează a fi înregistrate, expediate şi clasate la dosar, precum şi documentele de intrare executate se predau de către executanţi Subdiviziunii de protecţie.

233. În caz de necesitate, executanţii pot remite altor executanţi ai subdiviziunilor interioare respective, în timpul programului de muncă, documentele ce conţin informaţii atribuite la secret de stat, cu excepţia celor care au gradul de secretizare „Strict secret", dacă aceste documente îi priveşte nemijlocit şi le sînt adresate de către conducătorul autorităţii publice sau al altei persoane juridice ori de şeful subdiviziunii. În acest caz, restituirea documentului către executantul de la care a fost primit se va efectua în aceeaşi zi.

234. Remiterea unor astfel de documente de la un executant la altul se efectuează contra semnătură (recipisă) în Inventarul interior al documentelor care se află la executant (forma nr. 24, anexă la prezentul Regulament). De asemenea, conducătorii autorităţilor publice sau ai altor persoane juridice, precum şi şefii subdiviziunilor sînt obligaţi să semneze în inventarul interior pentru documentele primite de la executanţi.

235. Fiecare document sau alt purtător material de informaţii atribuite la secret de stat va fi inscripţionat cu numărul de înregistrare şi data cînd este înscris în registrul de evidenţă. Numerele de înregistrare sînt urmate de menţiunile „SS", „S", „C" sau „R", corespunzător gradului de secretizare atribuit.

236. Emitenţii şi deţinătorii de informaţii atribuite la secret de stat sînt obligaţi să înregistreze şi să ţină evidenţa tuturor documentelor şi materialelor primite, expediate sau a celor întocmite de unitatea proprie, potrivit legii.

237. Evidenţa actelor normative şi a celor cu caracter de dispoziţie emise de către autoritatea publică sau altă persoană juridică se efectuează conform registrului prevăzut în forma nr. 25, anexă la prezentul Regulament. Evidenţa actelor normative primite pentru informare sau executare de la autorităţile publice (hotărîri ale Parlamentului, decrete ale Preşedintelui, hotărîri şi dispoziţii ale Guvernului, acte emise de către alte autorităţi publice, inclusiv locale) se efectuează conform registrului prevăzut în forma nr. 26, anexă la prezentul Regulament.

238. Informarea cu conţinutul actelor normative şi de dispoziţie se efectuează contra semnătură (recipisă) pe o fişă specială, numai la indicaţia scrisă a conducătorului autorităţii publice sau al altei persoane juridice emitente.

239. În registrele de evidenţă a informaţiilor atribuite la secret de stat vor fi

menţionate numele şi prenumele persoanei care a primit documentul, iar aceasta va semna pentru primire.

240. Atribuirea numerelor de înregistrare în registrele de evidenţă se face consecutiv, pe parcursul unui an calendaristic. Numerele de înregistrare se înscriu obligatoriu pe toate exemplarele documentelor sau materialelor care conţin informaţii atribuite la secret de stat, precum şi pe documentele anexate.

241. Anual, documentele se clasează în dosare, potrivit problematicii, termenelor de păstrare stabilite în nomenclatoarele departamentale detaliate de informaţii care urmează a fi secretizate, precum şi altor criterii.

242. Clasarea documentelor sau altor purtători materiali de informaţii atribuite la secret de stat se face separat, în funcţie de suportul şi formatul acestora, cu folosirea mijloacelor de păstrare şi protejare adecvate.

243. Informaţiile avînd gradul de secretizare „Strict secret" şi cele cu privire la mobilizare vor fi compartimentate fizic şi păstrate separat de celelalte informaţii.

244. Atribuirea aceluiaşi număr de înregistrare unor documente cu conţinut diferit este interzisă.

245. Registrele de evidenţă vor fi completate de persoanele desemnate care deţin autorizaţie de acces la secret de stat de forma corespunzătoare.

Secţiunea a 3-a

Evidenţa caietelor de lucru şi pentru stenografiere, carnetelor de notiţe speciale, formularelor, mapelor de lucru, servietelor şi valizelor speciale

246. Caietele de lucru şi pentru stenografiere, carnetele de notiţe speciale se eliberează executanţilor pentru efectuarea însemnărilor ce conţin informaţii atribuite la secret de stat. Evidenţa acestora se ţine în Registrul de evidenţă a caietelor de lucru, potrivit formei nr. 27, anexă la prezentul Regulament. Evidenţa caietelor de lucru, pentru stenografiere şi a carnetelor de notiţe speciale poate fi efectuată într-un registru unic, însă în mod separat.

247. Ţinerea caietelor de lucru pentru înscrierea informaţiilor avînd gradul de secretizare „Strict secret" se efectuează doar cu permisiunea scrisă a conducătorilor autorităţilor publice sau altor persoane juridice.

248. Filele caietelor trebuie să fie şnuruite, numerotate, sigilate şi semnate de către şeful Subdiviziunii de protecţie. Caietele se secretizează, pe copertele acestora se indică destinaţia lor, numele, prenumele executantului şi numărul de înregistrare.

249. Filele carnetelor de notiţe speciale şi cotorul acestora se numerotează, iar pe fiecare filă se indică numărul de evidenţă al carnetului. În cazul editării caietelor de notiţe speciale cu fişe de control, cotoarele acestora nu se

numerotează.

250. La eliberarea carnetelor de notiţe speciale pentru unică utilizare, persoana din cadrul Subdiviziunii de protecţie va indica în Fişa de evidenţă a documentelor (dosarelor) eliberate (forma nr. 28, anexă la prezentul Regulament) numărul de file existente şi numărul de file rămase la restituirea carnetului. Consemnarea cu privire la transmiterea şi distrugerea filelor detaşabile se efectuează pe cotoarele filelor detaşate sau pe fişa de control a carnetului de notiţe special.

251. Carnetele de notiţe speciale, eliberate pentru unică utilizare, trebuie să fie prevăzute cu un suport rigid care exclude posibilitatea de imprimare a amprentelor documentului întocmit.

252. Inventarele interioare broşate ale documentelor care se află la executanţi se iau în evidenţă în Registrul de evidenţă a caietelor de lucru sau în conturile personale (forma nr. 29, anexă la prezentul Regulament). Conturile personale se iau în evidenţă în registre separate, conform modelului din forma nr. 27, anexă la prezentul Regulament.

253. Mapele de lucru, servietele şi valizele speciale se eliberează executanţilor contra semnătură (recipisă). La restituirea acestora Subdiviziunii de protecţie, se verifică corectitudinea sigilării lor şi respectarea termenului de restituire.

254. În lipsa executanţilor, în caz de necesitate, mapele de lucru, servietele şi valizele speciale pot fi deschise, cu permisiunea şefului Subdiviziunii de protecţie, de către angajaţii Subdiviziunii de protecţie, în prezenţa unui reprezentant al subdiviziunii în care activează executantul. Aceste persoane fac înscrieri, confirmate prin semnătură (recipisă), în inventarele interioare ale documentelor ce se află la executanţi sau într-un registru special, ţinut de Subdiviziunea de protecţie, indicînd cine, cînd şi cu ce scop a efectuat deschiderea, corespunderea documentelor cu inventarul interior, numărul ştampilelor cu care a fost şi cu care urmează a fi sigilată mapa de lucru, servieta sau valiza specială. În cazul în care este necesară extragerea documentelor din mapa de lucru, servieta sau valiza specială se indică numărul documentelor extrase şi numărul de file al acestora. După deschidere, mapa de lucru, servieta sau valiza specială, se sigilează cu ştampila personală a reprezentantului subdiviziunii în care activează executantul. La întoarcere, executantul este obligat să verifice prezenţa documentelor.

255. Pentru sigilarea mapelor de lucru, servietelor sau valizelor speciale, a depozitelor de păstrare a documentelor, executanţilor li se eliberează, contra semnătură (recipisă) în contul personal sau în Registrul de evidenţă a ştampilelor (forma nr. 30, anexă la prezentul Regulament), ştampile de metal numerotate.

Secţiunea a 4-a

Transmiterea informaţiilor atribuite la secret de stat

256. La transmiterea informaţiilor atribuite la secret de stat se va asigura respectarea principiului necesităţii de a lucra cu astfel de informaţii.

257. Transmiterea informaţiilor atribuite la secret de stat între autorităţile publice, alte persoane juridice sau cetăţeni se va efectua cu permisiunea autorităţii publice cu împuterniciri de dispoziţie asupra acestora.

258. Transmiterea informaţiilor atribuite la secret de stat, în procesul de elaborare şi adoptare a actelor normative poate fi efectuată fără permisiunea emitentului acestor informaţii, în limitele necesare îndeplinirii cerinţelor de tehnică legislativă.

259. La transmiterea informaţiilor atribuite la secret de stat vor fi create, în mod obligatoriu, condiţii necesare pentru protecţia acestor informaţii. În acest sens:

1) autorităţile publice trebuie să îndeplinească cerinţele prevăzute în articolul 32 alineatul (3) literele a) – e) din Lege;

2) alte persoane juridice, cu excepţia autorităţilor publice, trebuie să dispună de certificat de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor avînd un anumit grad de secretizare;

3) cetăţenii trebuie să dispună de dreptul de acces la informaţiile atribuite la secret de stat, de forma corespunzătoare.

260. Predarea-primirea informaţiilor atribuite la secret de stat între expeditor şi destinatar se face cu respectarea măsurilor de protecţie, prevăzute în prezentul Regulament.

261. Corespondenţa secretă se transmite numai prin Subdiviziunile de protecţie ale autorităţilor publice sau ale altor persoane juridice.

262. La primirea documentelor ce urmează a fi transmise, persoana din cadrul Subdiviziunii de protecţie verifică prezenţa tuturor exemplarelor şi filelor documentelor, ciornelor, corespunderea numerelor de înregistrare de pe documente cu numerele din registrele de evidenţă, corectitudinea întocmirii documentelor, prezenţa anexelor.

263. Documentele pot fi transmise destinatarilor cu sau fără scrisoare de însoţire.

264. La transmiterea documentelor cu scrisoare de însoţire, întocmirea lor se efectuează în modul prevăzut de punctele 191-192 ale prezentului Regulament.

265. Dacă anexele se transmit către destinatari diferiţi, enumerarea lor se face pentru fiecare destinatar în parte.

266. Dacă la expeditor nu rămîn copii (exemplare) ale anexelor transmise, atunci în scrisoarea de însoţire se face menţiunea „Numai destinatarului”.

267. Evidenţa documentelor întocmite se efectuează în registrele de evidenţă a documentelor întocmite (formele nr. 31 şi nr. 32, anexă la prezentul Regulament).

268. La transmiterea unui număr mare de anexe prin scrisoare de însoţire, dacă enumerarea acestora în registrele de evidenţă a documentelor întocmite este imposibil de efectuat, în rubrica „Tipul şi conţinutul succint al documentului” se va indica, în litere, numărul total de file al anexelor.

269. Documentele pot fi transmise destinatarilor fără scrisoare de însoţire, dacă conţinutul şi destinaţia acestora nu necesită explicaţii suplimentare.

270. La transmiterea documentelor fără scrisori de însoţire, pe plicurile în care se pun astfel de documente se înscriu numerele de înregistrare ale tuturor documentelor, indicîndu-se numărul de exemplare, iar în registrele de evidenţă se înscrie numărul şi data expedierii. Transmiterea documentelor ce se referă la mobilizare se face în plicuri aparte, separat de alte documente secretizate.

271. Toate documentele ce conţin informaţii atribuite la secret de stat se transmit către alte autorităţi publice sau alte persoane juridice în plicuri sigilate, opace şi rezistente.

272. Pe verso plicului, în centru se lipeşte eticheta de hîrtie cu amprenta de cauciuc „Pentru plicuri”, în aşa fel ca ea să cuprindă toate colţurile la mijloc.

273. Etichetele trebuie să fie confecţionate din hîrtie subţire care nu se supune stratificării, iar mărimea acestora trebuie să depăşească cu 3-4 mm diametrul amprentei ştampilei de cauciuc. Deasupra etichetelor se aplică un strat subţire de clei, care trebuie să depăşească marginile etichetei de hîrtie.

274. Pe plic se indică următoarele date:

1) parafa de secretizare – în colţul drept de sus;

2) după caz, menţiunea „Personal” sau litera „M” – sub parafa de secretizare;

3) semnătura persoanei care a efectuat împachetarea şi ştampila „Pentru plicuri”;

4) după caz, menţiunea „Urgent”, legalizată prin ştampila „Pentru plicuri” – în partea de sus în centrul plicului;

5) adresa destinatarului;

6) adresa expeditorului;

7) numerele de înregistrare a documentelor ce se conţin în plic.

275. La transmiterea unui document în mai multe exemplare, fără scrisoare de însoţire, în afara numărului de înregistrare al documentului, între paranteze, se indică numerele exemplarelor.

276. Documentele avînd gradele de secretizare „Strict secret”, „Secret” şi „Confidenţial” se transmit către alte autorităţi publice sau alte persoane juridice în plicuri duble. În acest caz, pe plicul exterior, în colţul stîng de sus se face înscrierea de preîntîmpinare „Plic dublu”. Parafa de secretizare, din punctul de

vedere al securităţii, nu trebuie, în nici un caz, să apară pe plicul exterior.

277. La împachetarea dublă, pe plicul interior pot fi indicate şi alte date, inclusiv menţiunile restrictive, numele expeditorului şi al destinatarului.

278. Transmiterea şi distribuirea corespondenţei secretizate se efectuează de către curieri speciali, în conformitate cu prevederile Legii Serviciului de Stat de Curieri Speciali nr. 402-XV din 2 decembrie 2004 şi ale Regulamentului Serviciului de Stat de Curieri Speciali, aprobat prin Hotărîrea Guvernului nr. 635 din 29 iunie 2005 „Cu privire la Serviciul de Stat de Curieri Speciali".

279. Conducătorii autorităţilor publice şi ai altor persoane juridice deţinătoare de informaţii atribuite la secret de stat vor desemna cel puţin o persoană din cadrul Subdiviziunii de protecţie proprii pentru transmiterea şi executarea operaţiunilor de predare-primire a corespondenţei secretizate, între acestea şi Serviciul de Stat de Curieri Speciali.

280. În caz de necesitate, cu permisiunea scrisă a conducătorului autorităţii publice sau al altei persoane juridice, documentele secretizate, cu excepţia celor care au gradul de secretizare „Strict secret", pot fi transmise în raza localităţii respective de către angajaţii Subdiviziunii de protecţie, desemnaţi în conformitate cu punctul 279 din prezentul Regulament, în serviete speciale, sigilate cu ştampila Subdiviziunii de protecţie şi numai însoţiţi de transportul departamental. Transmiterea şi distribuirea corespondenţei avînd gradul de secretizare „Strict secret" de către angajaţii desemnaţi ai Subdiviziunii de protecţie în raza localităţii respective se admite, doar în cazuri excepţionale, cu asigurarea pazei corespunzătoare (înarmate).

281. Transmiterea şi distribuirea corespondenţei secretizate de către angajaţii desemnaţi ai Subdiviziunii de protecţie, în afara localităţii respective, se admite, doar în cazuri excepţionale, cu asigurarea pazei corespunzătoare (înarmate).

282. În interiorul aceleiaşi clădiri sau al unui grup de clădiri, documentele ce conţin informaţii atribuite la secret de stat pot fi transmise într-un singur plic închis, menţionînd numai numele destinatarului, cu condiţia ca expedierea (distribuirea) să fie efectuată de persoana desemnată din cadrul Subdiviziunii de protecţie, care dispune de acces la secretul de stat de forma corespunzătoare.

283. Predarea-primirea corespondenţei în procesul transmiterii şi distribuirii se face contra semnătură (recipisă), în conformitate cu formele respective de evidenţă.

Secţiunea a 5-a

Recepţionarea şi înregistrarea informaţiilor atribuite la secret de stat

284. Toată corespondenţa secretizată, parvenită în autorităţile publice sau alte persoane juridice în timpul programului de muncă este recepţionată numai de către Subdiviziunea de protecţie.

285. În afara programului de muncă, corespondenţa secretizată este recepţionată de către persoanele de serviciu din cadrul autorităţii publice sau al altei persoane juridice, care înregistrează plicurile în Registrul de evidenţă a plicurilor (forma nr.33, anexă la prezentul Regulament), fără a le deschide. Corespondenţa recepţionată în acest mod se transmite, neîntîrziat, Subdiviziunii de protecţie, contra semnătură (recipisă).

286. Distribuirea corespondenţei secretizate, în afara programului de muncă, către autorităţile publice sau alte persoane juridice care nu dispun permanent de persoane de serviciu nu se efectuează.

287. La recepţionarea corespondenţei se verifică: corectitudinea adresei, integritatea ambalajului (plicului) şi amprentele ştampilei, corespunderea lor denumirii expeditorului, corespunderea numerelor indicate pe plic cu numerele indicate în registrul (borderoul, inventarul) de distribuire.

288. În cazul constatării unor nereguli (spre exemplu, deteriorarea ambalajului, necorespunderea amprentelor ştampilei cu denumirea expeditorului), plicul este recepţionat prin întocmirea unui proces-verbal, semnat de persoana care a distribuit plicul şi de cea care l-a recepţionat, fapt ce se consemnează în registru.

289. Un exemplar al procesului-verbal se remite, după caz, Serviciului de Stat de Curieri Speciali sau expeditorului pentru luarea măsurilor necesare.

290. Dacă plicul este deteriorat astfel încît permite divulgarea conţinutului documentelor pe care le conţine, plicul cu documentele respective se va păstra intact, iar despre acest fapt va fi informat neîntîrziat conducătorul autorităţii publice sau al altei persoane juridice şi Serviciul de Informaţii şi Securitate.

291. Persoana care recepţionează corespondenţa semnează lizibil în registrul (borderoul, inventarul) de distribuire, indicînd prin litere numărul plicurilor recepţionate, data, ora recepţionării lor şi legalizează semnătura sa prin ştampila respectivă. Ulterior, în registrul de evidenţă a plicurilor sau în Registrul de control al plicurilor (forma nr. 34, anexă la prezentul Regulament) se indică numărul de expediţie şi se scrie prin litere numărul plicurilor recepţionate. Persoana de serviciu indică suplimentar în registrul de evidenţă a plicurilor numărul documentelor indicat pe plicuri. Aceste înscrieri se confirmă prin semnătura curierului special care a distribuit corespondenţa, indicînd data şi ora de predare a corespondenţei.

292. Toate plicurile recepţionate şi înregistrate în registrul de control al plicurilor se remit contra semnătură (recipisă) şefului Subdiviziunii de protecţie sau persoanei împuternicite pentru a fi deschise. La deschiderea plicurilor se verifică corespunderea numerelor de înregistrare indicate pe ele cu numerele indicate pe documentele din plic, numărul documentelor cu datele de evidenţă indicate în scrisoarea de însoţire, numărul de exemplare şi de file ale tuturor documentelor.

293. Dacă plicul conţine mai multe documente, fiecare dintre ele se înregistrează cu un număr separat.

294. Persoana care deschide plicurile trebuie să se convingă de faptul că a extras toată corespondenţa din ele.

295. După deschiderea plicului, documentele se înregistrează neîntîrziat în Registrul de evidenţă a documentelor recepţionate sau în Fişele de evidenţă a documentelor recepţionate (formele nr. 35 şi nr. 36, anexă la prezentul Regulament) ori, respectiv, în formele de evidenţă ale documentaţiei tehnice.

296. Plicurile cu menţiunea „Personal" se deschid doar de către destinatar sau de persoana împuternicită. Înscrierea datelor referitoare la document se efectuează din spusele persoanei care a deschis plicul. În Registrul de evidenţă a documentelor recepţionate (formele nr. 35 şi nr. 36, anexă la prezentul Regulament) se face înscrierea „Plic cu menţiunea „Personal". După ce a luat cunoştinţă de conţinutul documentului, destinatarul acestuia restituie documentul în plic Subdiviziunii de protecţie. Documentele cu menţiunea „Personal" se păstrează în plic sigilat de către Subdiviziunea de protecţie. Ulterior, la decăderea necesităţii de a păstra documentele cu menţiunea „Personal", acestea se distrug în modul stabilit de prezentul Regulament.

297. În cazurile în care se constată necorespunderi în datele de evidenţă ale documentelor recepţionate, acestea vor fi menţionate într-un proces-verbal, întocmit în două exemplare, semnat de şeful şi persoana respectivă din cadrul Subdiviziunii de protecţie. Un exemplar al procesului-verbal împreună cu recto plicului în care au fost primite documentele se expediază Subdiviziunii de protecţie a autorităţii publice sau al altei persoane juridice expeditoare, iar celălalt exemplar se clasează în dosar.

298. La primirea procesului-verbal, Subdiviziunea de protecţie a autorităţii publice sau al altei persoane juridice expeditoare întreprinde măsurile necesare în vederea explicării şi lichidării necorespunderilor indicate în procesul-verbal.

299. Documentele expediate greşit se restituie expeditorului sau, de comun acord cu acesta, se expediază conform destinaţiei, în plicuri noi, pe care se vor indica numerele lor de înregistrare, anexînd recto plicului expeditorului, iar în registrul de control al plicurilor se înscrie numărul acestuia şi data expedierii.

300. Numărul de înregistrare a documentelor recepţionate se indică în mod obligatoriu în Registrul de control al plicurilor.

301. La înregistrarea documentelor recepţionate, în partea inferioară a primei pagini se aplică ştampila, în care se indică denumirea autorităţii publice sau al altei persoane juridice, numărul de evidenţă (de intrare), data înregistrării, numărul de file ale documentului de bază şi ale anexelor la acesta (filele anexelor nesecretizate se indică separat). Pe prima filă a anexelor se aplică ştampila „La nr.____ de intrare", indicîndu-se anul de înregistrare.

302. Documentele recepţionate de la structurile subordonate sau interioare, ce dispun de Subdiviziuni de protecţie, care au fost semnate de către conducătorii autorităţilor publice, altor persoane juridice sau organelor ierarhic superioare, pot fi transmise destinatarului cu numărul de înregistrare atribuit conform Registrului de evidenţă a documentelor, indicat în forma nr. 37, anexă la prezentul Regulament.

303. Ediţiile, materialele broşate, alte documente parvenite fără scrisori de însoţire trec în evidenţă în Registrul de control al plicurilor, în care se înscriu numerele de inventar sau alte numere de evidenţă, atribuite acestor documente la înregistrarea lor în registrele respective.

304. În cazul în care anexele nu pot fi clasate în dosar (spre exemplu, broşurile, documentele de format mare), se efectuează inventarierea lor, cu menţiunea respectivă în scrisorile de însoţire şi în registrele de evidenţă a documentelor recepţionate, iar scrisorile de însoţire se clasează în dosar. Anexele nesecretizate la documente, dacă nu se păstrează în comun, vor fi remise la secretariat, contra semnătură (recipisă) în Registrul de evidenţă a documentelor recepţionate, efectuîndu-se consemnarea respectivă pe scrisoarea de însoţire.

305. Documentele recepţionate, luate în evidenţa corespunzătoare, se remit, contra semnătură (recipisă), conducătorului autorităţii publice sau al altei persoane juridice căreia îi sînt adresate spre examinare.

306. Documentele avînd gradul de secretizare „Strict secret" se remit conducătorului autorităţii publice sau al altei persoane juridice, contra semnătură (recipisă), doar de către şeful Subdiviziunii de protecţie sau de persoana numită pentru îndeplinirea obligaţiilor acestuia.

307. Remiterea documentelor spre executare se efectuează numai prin intermediul Subdiviziunii de protecţie.

308. Remiterea documentelor neînregistrate spre executare nu se admite.

309. Documentele care au gradul de secretizare „Strict secret" pot fi aduse la cunoştinţă doar persoanelor care dispun de acest drept, în virtutea funcţiilor exercitate, numai în privinţa aspectelor legate nemijlocit de activitatea acestora şi doar cu permisiunea scrisă a conducătorului autorităţii publice, altei persoane juridice sau a persoanei căreia i-au fost adresate.

310. La primirea documentelor de la executanţi, angajaţii Subdiviziunii de protecţie verifică corespunderea numerelor de înregistrare respective şi a numărului de file ale documentelor cu menţiunile din registrul de evidenţă respectiv şi din Inventarul interior al documentelor care se află la executant, semnînd pentru recepţionarea documentelor.

Secţiunea a 6-a

Multiplicarea

311. Multiplicarea documentelor ce conţin informaţii atribuite la secret de stat se efectuează numai de către persoane autorizate să aibă acces la astfel de informaţii, în încăperi special destinate. Autorităţile publice sau alte persoane juridice care lucrează cu un volum neînsemnat de documente secrete pot efectua multiplicarea acestora în încăperea Subdiviziunii de protecţie.

312. Documentele secrete se multiplică într-un număr strict stabilit de exemplare şi se transmit numai acelor subdiviziuni, autorităţi publice sau alte persoane juridice, cărora le sînt necesare în procesul activităţii.

313. Multiplicarea documentelor secrete se face în baza Foii de comandă privind multiplicarea documentelor secrete, potrivit formei nr. 38, anexă la prezentul Regulament.

314. Se interzice multiplicarea documentelor secrete într-un număr de exemplare mai mare decît cel indicat în Foaia de comandă privind multiplicarea documentelor secrete, cu excepţia înlocuirii filelor rebutate.

315. Multiplicarea documentelor ce conţin informaţii atribuite la secret de stat, cu excepţia celor care au gradul de secretizare „Strict secret", se face în baza aprobării şefului subdiviziunii interioare, cu avizul Subdiviziunii de protecţie, ambele înscrise pe Foaia de comandă privind multiplicarea documentelor secrete.

316. Multiplicarea documentelor avînd gradul de secretizare „Strict secret" se face în baza aprobării conducătorului autorităţii publice sau al altei persoane juridice, cu avizul Subdiviziunii de protecţie, ambele înscrise pe foaia de comandă privind multiplicarea documentelor secrete.

317. La solicitare, multiplicarea documentelor ce conţin informaţii atribuite la secret de stat pentru alte autorităţi publice sau persoane juridice se poate efectua în baza Foii de comandă privind multiplicarea documentelor secrete, întocmite de către acestea. Executarea lucrărilor de multiplicare în asemenea cazuri se autorizează de către conducătorul autorităţii publice sau al persoanei juridice – executant, prin efectuarea înscrierii respective în Foaia de comandă privind multiplicarea documentelor secrete.

318. Foile de comandă privind multiplicarea documentelor secrete se înregistrează de către Subdiviziunea de protecţie în Registrul de evidenţă a foilor de comandă (forma nr. 39, anexă la prezentul Regulament). Pe foile de comandă privind multiplicarea documentelor secrete, parvenite de la alte autorităţi publice sau persoane juridice, se indică prin fracţie şi numărul de înregistrare al scrisorii de expediere.

319. Documentele secrete care urmează a fi multiplicate, împreună cu Foaia de comandă respectivă, se transmit, prin intermediul Subdiviziunii de protecţie,

către subdiviziunea de multiplicare, contra semnătură (recipisă), în formele corespunzătoare de evidenţă. Documentele se transmit doar pe termenul necesar îndeplinirii comenzii.

320. Subdiviziunile de multiplicare asigură înregistrarea documentelor primite şi a Foilor de comandă privind multiplicarea documentelor secrete ce le însoţesc în Registrul de evidenţă a documentelor secrete multiplicate (forma nr. 40, anexă la prezentul Regulament).

321. Pe documente, precum şi în registrele de evidenţă respective se fac menţiuni cu privire la data, numărul de copii sau de extrase efectuate, de pe care pagini sau părţi ale documentului, numărul de înregistrare a copiilor sau extraselor.

322. Consemnarea operaţiunii de multiplicare se face atît pe original, cît şi pe toate copiile rezultate. Pe documentul original menţiunea cu privire la multiplicare se aplică în partea de jos a ultimei pagini sau pe verso documentului original, indicîndu-se numărul copiilor făcute de pe el, data, numărul de înregistrare al acestora şi cui au fost expediate. Dacă numărul destinatarilor este mare, poate fi întocmit un tabel de distribuire, care se înregistrează ca document anexat la original.

323. Pe copiile rezultate în urma multiplicării, marcarea se aplică pe prima pagină, sub numărul de înregistrare al documentului, prin aplicarea menţiunii „Copie".

324. În cazul copierii succesive, la date diferite, a unui document secret, originalul va fi marcat la fiecare operaţiune, care va fi, de asemenea, înscrisă în registru. Exemplarele rezultate în urma copierii documentului secret se numerotează în ordine succesivă, chiar dacă operaţiunea se efectuează de mai multe ori şi la date diferite.

325. Extrasul dintr-un document care conţine informaţii atribuite la secret de stat se face în baza Foii de comandă privind multiplicarea documentelor secrete, analogic procedurii stabilite pentru multiplicare, iar documentul rezultat va avea menţionat sub numărul de exemplar cuvîntul „Extras" şi numărul de înregistrare al documentului original.

326. Multiplicarea documentelor parvenite de la alte autorităţi publice sau alte persoane juridice se face doar cu consimţămîntul conducătorului autorităţii publice sau al altei persoane juridice cu împuterniciri de dispoziţie asupra acestuia.

327. Parafa de secretizare atribuită unui document original se aplică, în mod identic, reproducerilor sau traducerilor.

328. Traducerea documentului se înregistrează cu acelaşi număr de înregistrare ca şi originalul documentului, efectuîndu-se înscrierea corespunzătoare în formele de evidenţă.

329. Dacă emitentul doreşte să aibă control exclusiv asupra reproducerii,

documentul va conţine o indicaţie vizibilă cu următorul conţinut: „Reproducere interzisă”.

330. Informaţiile atribuite la secret de stat, înscrise pe documente cu regim restrictiv de reproducere, care au menţiunea „Reproducerea interzisă”, nu se multiplică.

331. În cazul multiplicării unui document care conţine informaţii atribuite la secret de stat se procedează astfel:

1) se stabileşte numărul de exemplare în care va fi multiplicat;

2) se completează şi se aprobă, în modul stabilit, Foaia de comandă, după care aceasta se înregistrează în registrul de evidenţă a foilor de comandă;

3) documentul original, împreună cu Foaia de comandă, se predă subdiviziunii de multiplicare pe bază de semnătură (recipisă);

4) după verificarea exemplarelor rezultate, acestea, împreună cu documentul original şi Foaia de comandă, se predau, pe bază de semnătură (recipisă) în Registrul de evidenţă a documentelor secrete multiplicate, Subdiviziunii de protecţie în vederea distribuirii sau expedierii.

332. La finisarea operaţiunilor de multiplicare se vor întreprinde măsurile necesare în vederea excluderii posibilităţii de reproducere neautorizată a informaţiilor multiplicate, fapt consemnat în Foaia de comandă privind multiplicarea documentelor secrete sau în Registrul de evidenţă a documentelor secrete multiplicate.

333. Stenografierea, redactarea după dictare sau de pe dispozitivele de redare a sunetului documentelor ce conţin informaţii atribuite la secret de stat, cu excepţia celor avînd gradul de secretizare „Strict secret”, se efectuează numai în încăperi izolate, unde este exclusă posibilitatea de ascultare a conţinutului acestora de către persoanele neautorizate.

334. Înregistrările stenografice a informaţiilor atribuite la secret de stat, cu excepţia celor care au gradul de secretizare „Strict secret”, se efectuează numai în caietele pentru stenografiere.

335. Purtătorii de informaţii magnetici sau de altă natură, destinaţi pentru imprimarea informaţiilor atribuite la secret de stat, şi caietele pentru stenografiere se înregistrează în Registrul de evidenţă al caietelor de lucru, iar după finalizarea activităţii se predau spre păstrare Subdiviziunii de protecţie. Pe purtătorul de informaţii se aplică numărul de înregistrare.

336. Toţi purtătorii materiali de informaţii atribuite la secret de stat, utilizaţi în activitatea de multiplicare, pînă la transmiterea lor Subdiviziunii de protecţie sau pînă la distrugere, se păstrează în condiţii care să asigure protecţia corespunzătoare a secretului de stat (safeuri, dulapuri de metal, depozite speciale sigilate, alţi suporţi speciali).

Secţiunea a 7-a

Multiplicarea tipografică

337. Primirea documentelor secrete pentru multiplicare tipografică, evidenţa, păstrarea şi transmiterea ediţiilor secrete se efectuează prin intermediul Subdiviziunilor de protecţie sau al subdiviziunilor documentaţiei tehnice.

338. Documentele secrete primite spre multiplicare tipografică se înregistrează în Registrul de evidenţă a lucrărilor tipografice secrete (forma nr. 41, anexă la prezentul Regulament).

339. Tirajul ediţiilor secrete şi lista destinatarilor acestora se aprobă de către beneficiar, după coordonarea cu Subdiviziunea de protecţie a autorităţii publice cu împuterniciri de dispoziţie asupra informaţiei respective.

340. Ediţiile cu tiraj mare (spre exemplu: cărţi, instrucţiuni, broşuri) se tipăresc cu numerele de inventar atribuite originalelor acestora în Registrul de evidenţă a ediţiilor secrete (forma nr. 42, anexă la prezentul Regulament), pînă la predarea lor tipografiei. Dacă în ediţie sînt incluse mai multe documente care au numere de evidenţă separate, atunci acestei ediţii i se atribuie un număr unic de inventar.

341. Ordinele, instrucţiunile, indicaţiile şi alte acte cu caracter organizatoric şi de dispoziţie, precum şi documentaţia tehnică care se ţine în evidenţa de inventar se tipăresc cu numerele de evidenţă atribuite acestora.

342. Dacă într-o ediţie au fost incluse documente cu diferite grade de secretizare, atunci acestei ediţii i se aplică parafa de secretizare care corespunde celui mai înalt grad.

343. Pe copertă şi pe foaia de titlu a fiecărui exemplar al ediţiei (documentului) se indică: parafa de secretizare, numărul exemplarului şi numărul de inventar sau de evidenţă atribuit ediţiei (documentului). Pe verso ultimei file de text se înscrie o menţiune cu privire la: filele copertei pe care sînt indicate informaţii secrete, numărul de pagini, numărul planşelor (schemelor) nenumerotate.

344. Dacă ediţia secretă este formată din cîteva părţi (capitole, articole) cu diverse grade de secretizare, parafa de secretizare se aplică la începutul fiecărei dintre aceste părţi.

345. Dacă în ediţia secretă sînt incluse scheme, desene, hărţi, alte elemente componente de dimensiuni mai mari decît formatul ediţiei, atunci ele, de regulă, se plasează la sfîrşitul ediţiei, iar pe verso foii de titlu se indică numărul de planşe, numerele acestora şi numărul de file intercalate. Dacă planşele nu se plasează la sfîrşitul ediţiei, atunci se menţionează între care pagini au fost intercalate.

346. În cazul în care există un număr mare de planşe, acestea se broşează în blocuri separate, la sfîrşitul ediţiei sau în albume aparte.

347. Pe planşe se aplică parafa de secretizare respectivă, numărul comenzii tipografice şi anul de ediţie.

348. Evidenţa documentelor în tipografie se ţine conform Registrului de evidenţă a lucrărilor tipografice secrete.

349. Foaia de comandă privind multiplicarea documentelor secrete executate, împreună cu originalele documentelor, se transmit Subdiviziunii de protecţie sau subdiviziunii documentaţiei tehnice, în bază de semnătură (recipisă) în registrul de evidenţă a lucrărilor tipografice secrete.

350. Imprimările de corectură se iau în evidenţă în registre corespunzătoare, cu numerele de evidenţă a originalelor. Ele se expediază beneficiarilor, în modul stabilit, pentru transmiterea documentelor secrete.

351. Pînă la începutul paginării, şpalturile se păstrează de către persoana desemnată special în acest scop sau nemijlocit de către zeţar în regalurile pentru forme (dulapuri, safeuri), încuiate şi sigilate.

352. La finisarea lucrărilor, toate materialele secrete se pun în safeuri (dulapuri de metal) şi depozite, iar încăperile unde acestea se păstrează se verifică, se încuie, se sigilează şi se predau sub pază. La sfîrşitul schimbului, formele de zaţ care se află în maşinile de tipar se acoperă cu scuturi şi se sigilează.

353. La finisarea multiplicării tipografice a documentelor secrete, executanţii, împreună cu angajaţii Subdiviziunii de protecţie, verifică locurile de muncă şi tehnica de multiplicare pentru a exclude posibilitatea de a rămîne producţie tipărită secretă (inclusiv rebutată).

354. După executarea comenzii (obţinerea permisiunii de a publica ediţia) şi după verificarea corectitudinii textului ediţiei, tot materialul rebutat (imprimările de corectură, şpalturile, paginaţia, ultima corectură, matriţele) se verifică şi, de comun acord cu beneficiarul, se distrug în modul stabilit de prezentul Regulament.

355. Tirajele ediţiei tipărite se ţin în evidenţă în acelaşi registru în care au fost luate în evidenţă originalele cu numerele atribuite originalelor. Ediţiile secrete ale publicaţiilor cu tiraj mare, primite din alte autorităţi publice sau alte persoane juridice, se ţin în evidenţă în Registrul de evidenţă a ediţiilor secrete.

356. În cazul în care se depistează lipsa sau pierderea unor file (exemplare) în procesul de multiplicare tipografică a documentelor secrete, executantul informează imediat conducătorul tipografiei şi şeful Subdiviziunii de protecţie.

357. Completarea filelor sau a exemplarelor care lipsesc se efectuează cu permisiunea autorităţii publice cu împuterniciri de dispoziţie asupra informaţiilor respective, în baza Foii de comandă privind multiplicarea documentelor secrete,

aprobată în modul corespunzător.

358. Ediţiile şi documentele secrete editate, pînă la remiterea lor beneficiarului, se păstrează împachetate şi sigilate în safeuri sau în încăperi speciale.

359. Transmiterea documentelor (tirajului ediţiei) secrete multiplicate tipografic se efectuează în modul stabilit de prezentul Regulament, în conformitate cu lista de expediere, în care se enumără destinatarii şi numărul de exemplare expediate. În registrul de evidenţă a ediţiilor secrete se face o înscriere cu privire la data transmiterii documentelor şi locul de aflare a listei destinatarilor, cu indicarea numărului de înregistrare al acesteia.

Secţiunea a 8-a

Nomenclatorul dosarelor.

Clasarea documentelor şi dosarelor

360. În scopul întocmirii corecte a dosarelor, păstrării sigure a documentelor şi selectării lor urgente, se întocmeşte Nomenclatorul dosarelor (forma nr. 43, anexă la prezentul Regulament), ţinîndu-se cont de sarcinile şi funcţiile autorităţii publice sau ale altei persoane juridice.

361. În Nomenclatorul dosarelor se includ toate dosarele care reflectă activitatea autorităţii publice sau al altei persoane juridice, dosarele subdiviziunilor care activează provizoriu (spre exemplu, a comisiilor tehnice, a altor comisii), dosarele nefinalizate şi cele sosite din alte autorităţi publice sau alte persoane juridice pentru a fi continuate, precum şi Registrul unic de evidenţă al registrelor, dosarelor finalizate. Dosarele pe problemele care se soluţionează pe parcursul mai multor ani (dosare transmisibile) se introduc în Nomenclatorul dosarelor pe fiecare an, avînd acelaşi număr de ordine pe întreaga perioadă de timp necesară pentru soluţionarea acestor probleme, cu efectuarea menţiunii respective în Nomenclatorul dosarelor pe anul care a expirat: „Transmisibil, început în anul _____”.

362. Nomenclatoarele dosarelor se împart în nomenclatoare individuale (pentru documentele unei subdiviziuni interioare concrete) şi nomenclatoare de totalizare (formate din nomenclatoarele individuale ale subdiviziunilor interioare din autoritatea publică sau altă persoană juridică). Pentru persoanele juridice cu activitate economică şi documentaţie similară se întocmeşte într-un nomenclator-tip al dosarelor.

363. Nomenclatorul dosarelor se întocmeşte de către Subdiviziunea de protecţie în comun cu şefii subdiviziunilor interioare şi, după caz, şeful arhivei secrete a autorităţii publice sau al altei persoane juridice. Elaborarea Nomenclatorului dosarelor se efectuează în conformitate cu regulile stabilite de Serviciul de Stat de Arhivă, ţinîndu-se cont de importanţa documentelor, uniformitatea documentelor intrate la dosar, termenele lor de păstrare. În cazul unui număr mic de dosare secrete (pînă la zece), Nomenclatorul dosarelor poate

fi întocmit pentru cîţiva ani, însă nu mai mult de cinci.

364. Nomenclatorul dosarelor semnat de către şeful Subdiviziunii de protecţie, coordonat cu Serviciul de Stat de Arhivă şi aprobat de către conducătorul autorităţii publice sau al altei persoane juridice se aplică începînd cu 1 ianuarie al anului următor.

365. Nomenclatorul dosarelor se ţine în evidenţă conform Registrului de evidenţă a documentelor întocmite (formele nr. 31 şi nr. 32, anexă la prezentul Regulament) şi se păstrează pe parcursul anului la şeful Subdiviziunii de protecţie sau la persoana responsabilă de păstrarea lui. După efectuarea controlului anual, Nomenclatorul dosarelor se clasează într-un dosar, separat cu nomenclatoarele. Evidenţa nomenclatoarelor broşate se ţine în Registrul unic de evidenţă a registrelor şi dosarelor finalizate (forma nr. 22, anexă la prezentul Regulament).

366. Nomenclatorul dosarelor se întocmeşte în aşa fel încît fiecare executant să aibă posibilitatea a lua cunoştinţă de volumul informaţiilor secrete necesare pentru îndeplinirea obligaţiilor de serviciu.

367. În caz de necesitate, în Nomenclatorul dosarelor pot fi operate modificări şi completări, în ordinea stabilită pentru aprobarea acestuia.

368. Termenele de păstrare a dosarelor incluse în Nomenclatorul dosarelor se stabilesc conform listelor tip sau listelor departamentale desfăşurate ale documentelor ce conţin termenele de păstrare.

369. Volumele dosarelor şi registrelor se introduc în Nomenclatorul dosarelor pe măsura deschiderii lor, cu indicarea numelui executantului responsabil de întocmirea dosarului (volumului), registrului.

370. În Nomenclatorul dosarelor se fac înscrieri cu privire la data deschiderii şi finalizării dosarului (volumului), numărul de file şi alte date necesare. Dacă pe parcursul anului în autoritatea publică sau altă persoană juridică se deschid noi dosare, acestea se includ suplimentar în Nomenclatorul dosarelor. În acest scop, la fiecare capitol al Nomenclatorului dosarelor se rezervă numere. La expirarea anului, la sfîrşitul Nomenclatorului dosarelor se indică numărul de dosare (volume) deschise care se păstrează provizoriu şi care permanent şi numărul de dosare transmisibile pentru anul următor.

371. Nomenclatorul dosarelor reprezintă documentul de evidenţă principal pentru anul în curs şi constituie baza organizării evidenţei, conform Registrului unic de evidenţă a registrelor şi dosarelor finalizate (forma nr. 22, anexă la prezentul Regulament).

372. Numerele de ordine ale dosarelor, conform Nomenclatorului dosarelor, reprezintă numerele dosarelor respective. În cazul unui număr mare de dosare incluse în Nomenclatorul dosarelor, acestora li se pot atribui indici care se formează din semnele convenţionale ale subdiviziunii interioare şi numărul de

ordine al dosarelor (în limitele nomenclatorului dosarelor pentru subdiviziunea interioară).

373. Documentele se clasează în dosare pe diferite criterii (problematică, tip de documente, grad de secretizare, termen de păstrare, corespondenţă cu anumite autorităţi sau alte persoane juridice etc.). Întocmirea dosarelor se efectuează în conformitate cu regulile stabilite de Serviciul de Stat de Arhivă al Republicii Moldova.

374. Dosarele se întocmesc pe măsura clasării documentelor anului în curs. Dosarele transmisibile se întocmesc într-un număr strict limitat.

375. Documentele păstrate permanent se includ în dosare separat de cele păstrate provizoriu.

376. În dosare se clasează numai documentele executate şi întocmite corect. La recepţionarea documentelor executate pentru a fi clasate în dosare se verifică corectitudinea întocmirii acestora.

377. Pe coperta dosarului se va aplica: parafa de secretizare corespunzătoare gradului de secretizare a informaţiilor care se conţin în documentele clasate, denumirea autorităţii publice sau a altei persoane juridice (a subdiviziunii interioare), numărul dosarului, după caz, titlul dosarului, data, luna, anul deschiderii şi finalizării dosarului, numărul de file al acestuia, precum şi termenul de păstrare.

378. Data deschiderii şi finisării dosarului corespunde datei clasării primului şi ultimului document în dosar.

379. Concomitent cu dosarul se întocmeşte şi fişa de evidenţă privind eliberarea documentelor (dosarelor), conform formei nr. 28, anexă la prezentul Regulament, care se păstrează într-un plic lipit pe partea interioară a copertei dosarului şi se predă în arhivă împreună cu dosarul. La completarea deplină a fişei de evidenţă privind eliberarea documentelor (dosarelor) se întocmeşte o fişă nouă, care se anexează la cea completată şi se păstrează împreună cu dosarul.

380. Fişa completată se include în Inventarul interior al dosarului (forma nr. 44, anexă la prezentul Regulament), mai jos de însemnările totale, dar nu se consideră ca filă la dosar şi nu se numerotează.

381. Toate dosarele finisate trebuie să fie corect perfectate: filele dosarului trebuie să fie broşate, numerotate şi incluse în inventarul interior, iar pe inventar şi pe o filă specială cusută la sfîrşitul dosarului se face o înscriere de confirmare.

382. Toate documentele cusute la dosar se numerotează pe fiecare filă, în colţul drept de sus. Denumirea documentelor, numărul de evidenţă şi data acestora cu numărul de file se includ în inventarul interior al documentelor, care se află în dosar.

383. Filele inventarului interior se numerotează separat. Numărul acestora se va indica în menţiunea de confirmare, după numărul total de file ale dosarului.

384. După finalizarea dosarului, la sfîrşitul inventarului interior se indică, în cifre şi în litere, numărul documentelor incluse în el. De asemenea, se indică funcţia, numele, prenumele persoanei din cadrul Subdiviziunii de protecţie care a întocmit inventarul, iar pe fila specială cusută la sfîrşitul dosarului se efectuează o înscriere, în cifre şi în litere, privind numărul filelor cusute în el, conform modelului stabilit în forma nr. 44, anexă la prezentul Regulament.

385. Dosarul cu documente se coase, se sigilează şi se legalizează prin semnătura persoanei din cadrul Subdiviziunii de protecţie care l-a întocmit.

386. Sigilarea dosarului se efectuează cu ajutorul unei etichete de hîrtie cu amprentele ştampilei Subdiviziunii de protecţie, care se lipeşte în aşa mod încît să cuprindă aţele şireturilor cu care a fost cusut dosarul.

387. Fiecare dosar poate să conţină cel mult 250 de file. În cazul în care documentele clasate în dosar depăşesc acest număr, se întocmeşte un alt volum, indicîndu-se numărul lui de ordine.

388. Se interzice includerea în dosar a documentelor care nu se atribuie la acesta, a ciornelor, precum şi a documentelor care urmează a fi restituite.

389. Rectificările efectuate în inventarul interior al dosarului trebuie să fie legalizate prin semnăturile persoanei care-l întocmeşte şi a şefului Subdiviziunii de protecţie.

390. În vederea asigurării regimului secret, documentele, pe parcursul anului, pot fi păstrate în biblioraft sau în mape cu clape, iar la finele anului se clasează în dosar.

391. Pentru dosarele cu şine şi mapele cu clape se întocmeşte inventarul interior al documentelor care se află în ele şi foaia de titlu pe care se fac menţiunile stabilite de prezentul Regulament.

392. Eliberarea dosarelor sau a unor documente aparte, necesare în activitatea de serviciu, se efectuează de către Subdiviziunea de protecţie doar executanţilor care au drept de acces la acestea, contra semnătură (recipisă) în fişa de evidenţă privind eliberarea documentelor (dosarelor), în care se indică datele cu privire la dosarul sau documentul eliberat (numărul dosarului sau al documentului eliberat, numărul exemplarului documentului şi numărul de file al acestuia).

393. Dosarele şi documentele eliberate ce conţin informaţii cu gradul de secretizare „Strict secret" se restituie în aceeaşi zi.

394. Dacă este necesar ca executantul să ia cunoştinţă numai de conţinutul anumitor documente ce se află în dosar, care nu au legătură nemijlocită cu activitatea desfăşurată, informarea cu aceste documente se face cu permisiunea scrisă a şefului subdiviziunii în care lucrează executantul, în prezenţa unei persoane din cadrul Subdiviziunii de protecţie.

395. Lucrul cu documentele şi dosarele avînd gradul de secretizare „Strict secret” se efectuează în condiţii care asigură păstrarea acestora şi exclud posibilitatea de acces al altor persoane la conţinutul lor.

396. Retragerea din dosar a documentelor sau transferarea acestora dintr-un dosar în altul se efectuează, în cazuri excepţionale, numai cu permisiunea şefului Subdiviziunii de protecţie, prin anexarea în dosarul respectiv a unei Adeverinţe de substituire, în conformitate cu forma nr. 45, anexă la prezentul Regulament. În cazul în care din dosar se retrag definitiv unele documente, în inventarul interior al dosarului şi în formele de evidenţă se vor face menţiunile respective.

397. La retragerea documentelor din dosarele înregistrate în registrele de evidenţă ale anilor precedenţi, acestea trebuie înregistrate din nou în registrele de evidenţă a documentelor secrete ale anului în curs, cu efectuarea menţiunilor respective în adeverinţa de substituire.

398. Adeverinţa de substituire este semnată de către şeful Subdiviziunii de protecţie.

399. Menţiunile cu privire la modificarea numărului de file ale dosarului la retragerea definitivă a documentelor din acesta se indică pe copertă, în inventarul interior şi pe fila specială de confirmare.

400. La retragerea definitivă a documentelor din dosar, renumerotarea filelor acestuia nu se efectuează.

401. Toate dosarele finisate se ţin în evidenţă în Registrul unic de evidenţă al registrelor, dosarelor finalizate.

402. În cazul în care dosarul conţine mai multe volume, fiecare dintre acestea se înregistrează în Registrul unic de evidenţă a registrelor, dosarelor finalizate, cu un număr aparte, care se aplică pe copertă.

403. În Registrul unic de evidenţă a registrelor, dosarelor finalizate se fac menţiuni cu privire la data deschiderii şi finisării dosarului, termenele de păstrare, numărul de file ale acestuia, după caz alte date necesare.

404. Dosarele finisate se transmit pentru păstrare în arhivă. Despre predarea dosarului în arhivă sau, eventual, distrugerea acestuia se va indica în Registrul unic de evidenţă a registrelor şi dosarelor finalizate.

405. Autorităţile publice sau alte persoane juridice care deţin informaţii atribuite la secret de stat vor organiza şi vor efectua expertiza valorii documentelor în vederea predării acestora spre păstrare în arhivele secrete departamentale sau pentru distrugere. În acest sens, în autorităţile publice sau alte persoane juridice se creează comisii de expertiză, formate din cel puţin 3 membri.

406. Pentru păstrarea documentelor finisate, în autorităţile publice sau alte persoane juridice se creează arhive secrete departamentale, subordonate

Subdiviziunilor de protecţie, care trebuie să asigure selectarea, evidenţa, păstrarea şi utilizarea documentelor Fondului Arhivistic al Republicii Moldova, constituite ca urmare a activităţii lor şi a subdiviziunilor subordonate.

407. Dosarele finisate se păstrează cel puţin un an în Subdiviziunea de protecţie, după care se transmit în arhiva secretă departamentală, în baza inventarelor întocmite în acest sens. Un exemplar al inventarului cu recipisa de la arhivă pentru primirea dosarelor se restituie depunătorului şi se păstrează în Subdiviziunea de protecţie.

408. La predarea-primirea documentelor în arhiva secretă departamentală se verifică corectitudinea întocmirii şi selectării acestora. Documentele, dosarele şi inventarele la a căror întocmire s-au admis încălcări, urmează a fi rectificate de către persoanele responsabile pentru predarea documentelor în arhivă.

409. Documentele se păstrează în arhivele secrete departamentale pe parcursul termenului de secretizare a acestora.

410. La expirarea termenului de secretizare, documentele desecretizate care prezintă valoare istorică, ştiinţifică, culturală se transmit spre păstrare permanentă la Arhiva Naţională a Republicii Moldova, în modul stabilit de legislaţia în vigoare.

411. La dosarele selectate pentru păstrarea permanentă se întocmesc inventare, care vor fi aprobate de către comisiile de expertiză şi control ale instituţiilor de arhivă respective. Inventarele dosarelor care se vor păstra temporar se întocmesc separat de inventarele dosarelor care vor fi păstrate permanent. Aceste inventare se întocmesc în două exemplare şi nu se expediază în instituţiile de arhivă.

412. În cazul reorganizării sau lichidării autorităţii publice sau altei persoane juridice, pentru soluţionarea chestiunilor privind păstrarea ulterioară a documentelor Fondului arhivistic de stat se instituie o comisie, în componenţa căreia vor intra inclusiv reprezentanţi ai organului de stat pentru supravegherea şi administrarea Fondului Arhivistic al Republicii Moldova şi angajaţi ai Subdiviziunii de protecţie.

413. Documentele şi dosarele secretizate, păstrate provizoriu la expirarea termenelor stabilite, se distrug în modul prevăzut de prezentul Regulament.

414. Angajaţii arhivei fondurilor secrete întocmesc schema amplasării documentelor şi dosarelor şi planul evacuării lor în situaţii excepţionale. Schema şi planul se coordonează cu şeful Subdiviziunii de protecţie şi se aprobă de către conducătorul arhivei.

415. Evidenţa şi păstrarea documentelor şi dosarelor în arhiva secretă departamentală se efectuează în conformitate cu regulile de activitate a Arhivei de Stat şi cu prezentul Regulament.

416. Documentele şi dosarele, cu excepţia celor avînd gradul de secretizare

„Strict secret” care se păstrează în arhivele secrete departamentale, pot fi eliberate pentru utilizare temporară executanţilor care au acces la secretul de stat, cu permisiunea şefilor subdiviziunilor lor interioare şi Subdiviziunii de protecţie. Dosarele se eliberează executanţilor la locul de muncă în cazuri excepţionale, în baza fişei de evidenţă privind eliberarea documentelor (dosarelor).

417. Documentele de arhivă şi dosarele care au gradul de secretizare „Strict secret” nu se eliberează executanţilor la locul de muncă. Informarea cu conţinutul unor astfel de documente se efectuează în încăperea arhivei sau Subdiviziunii de protecţie, cu permisiunea şefului Subdiviziunii de protecţie şi a conducătorului autorităţii publice sau al altei persoane juridice.

418. Controlul disponibilului de documente secrete în arhivele secrete departamentale se efectuează cel puţin o dată la 5 ani.

419. Modificarea parafei de secretizare şi desecretizarea documentelor şi dosarelor, care se păstrează în arhiva secretă departamentală, se efectuează în modul stabilit de prezentul Regulament.

420. Despre modificarea parafei de secretizare sau desecretizarea documentelor şi dosarelor, care se află la păstrare în arhiva secretă departamentală se fac menţiunile respective pe acestea, indicîndu-se numărul şi data deciziei cu privire la modificarea parafei de secretizare sau cu privire la desecretizare.

421. Dosarele desecretizate se transmit pentru păstrare obişnuită, conform actului de inventar, cu efectuarea menţiunilor respective în formele de evidenţă a documentaţiei din arhivă.

422. Modificarea parafei de secretizare a documentelor secrete selectate pentru arhivele de stat se efectuează de către arhivele de stat împreună cu autorităţile publice sau cu alte persoane juridice şi, după caz, cu succesorii lor de drept, ale căror documente se păstrează în arhive.

423. Desecretizarea purtătorilor materiali de informaţii atribuite la secret de stat care se păstrează în fondurile închise ale arhivelor se efectuează de către conducătorii arhivelor de stat, cu condiţia că organizaţia întemeietoare a fondului sau succesorul ei de drept le deleagă astfel de împuterniciri. În caz de lichidare a organizaţiei întemeietoare a fondului şi de lipsă a succesorului ei de drept, problema desecretizării purtătorilor materiali de informaţii atribuite la secret de stat este examinată de către Comisia interdepartamentală pentru protecţia secretului de stat.

424. Documentele şi dosarele avînd gradul de secretizare „Strict secret”, care se află la păstrare de stat, pot fi eliberate pentru utilizare provizorie cetăţenilor care dispun de dreptul de acces la secret de stat, autorităţilor publice sau altor persoane juridice care deţin certificat de securitate, cu permisiunea autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii, care a predat aceste documente şi dosare la păstrare, sau a succesorilor acestora.

Secţiunea a 9-a

Bibliotecile secrete

425. Pentru asigurarea specialiştilor cu informaţie tehnico-ştiinţifică şi cu altă informaţie secretă, în autorităţile publice sau alte persoane juridice pot fi create biblioteci ale ediţiilor, documentaţiei tehnico-ştiinţifice şi a microhărţilor secrete.

426. Pentru bibliotecile secrete se eliberează încăperi speciale, care trebuie să dispună de depozite, săli de lectură dotate cu locuri de lucru pentru executanţi (abonaţi), separate prin pereţi despărţitori de protecţie, cu ferestre (bariere) pentru eliberarea şi restituirea documentelor, care ar permite supravegherea vizuală a executanţilor (abonaţilor) cărora li s-au eliberat documente secrete.

427. Se interzice păstrarea documentelor avînd gradul de secretizare „Strict secret" în bibliotecile secrete ale autorităţilor publice sau ale altor persoane juridice.

428. Evidenţa documentelor din bibliotecile secrete se ţine de către Subdiviziunea de protecţie sau reprezentantul acesteia în Registrul de evidenţă a ediţiilor secrete sau în Registrul de evidenţă a materialelor broşate (forma nr. 46, anexă la prezentul Regulament).

429. Documentele secrete se eliberează pentru utilizare în sala de lectură executanţilor (abonaţilor), care dispun de dreptul de acces la acestea, la prezentarea permisului scris (cu indicarea tematicii sau a denumirii ediţiei, documentului), eliberat de şeful subdiviziunii interioare respective şi vizată de şeful Subdiviziunii de protecţie.

430. Documentele pot fi eliberate executanţilor (abonaţilor) la locul de muncă, în cazuri excepţionale, cu respectarea cerinţelor prezentului Regulament.

431. Eliberarea documentelor se face contra semnătură (recipisă) în Fişa de evidenţă privind eliberarea documentelor (dosarelor).

432. Însemnările necesare de pe documentele eliberate se efectuează în caiete de lucru ţinute la evidenţă.

433. Pentru fiecare executant (abonat) care utilizează serviciile bibliotecii secrete se întocmeşte o fişă în care se introduc numerele de evidenţă a documentelor eliberate acestuia.

434. Eliberarea documentelor din bibliotecile secrete reprezentanţilor altor autorităţi publice sau persoane juridice se efectuează la prezentarea dispoziţiei eliberate abonatului de aceste autorităţi publice sau al persoanei juridice, a certificatului de acces la secret de stat de forma corespunzătoare şi a permisului scris, eliberat de conducătorul autorităţii publice sau al persoanei juridice în gestiunea căreia se află biblioteca sau de şeful subdiviziunii interioare care a primit reprezentantul menţionat. Aceşti abonaţi fac înscrieri necesare numai în

caietele de lucru luate în evidenţă. La finisarea lucrului cu documentele secrete eliberate, aceste înscrieri se examinează şi se vizează de şeful subdiviziunii interioare respective, caietele fiind predate Subdiviziunii de protecţie pentru transmiterea lor conform destinaţiei, în modul stabilit de prezentul Regulament.

435. Controlul asupra disponibilului documentelor în bibliotecile secrete şi asupra respectării regulilor de utilizare a acestora se efectuează cel puţin o dată în an, în modul stabilit de prezentul Regulament, de către comisii special instituite în acest scop.

Secţiunea a 10-a

Distrugerea purtătorilor materiali de informaţii atribuite la secret de stat

436. Sînt supuse distrugerii purtătorii materiali de informaţii atribuite la secret de stat care şi-au pierdut importanţa practică sau al căror termen de secretizare a expirat şi nu au valoare istorică sau altă valoare.

437. Distrugerea documentelor şi a altor purtători materiali de informaţii atribuite la secret de stat (în continuare – materiale) se face pe calea arderii, topirii, fragmentării (în fragmente cu suprafaţa de cel mult 2,5 mm2), dizolvării sau descompunerii chimice, transformării într-o masă moale fără formă sau praf, prin alte metode, astfel încît să nu mai poată fi reconstituite.

438. Documentele şi dosarele avînd gradul de secretizare „Strict secret" se distrug numai prin ardere.

439. Selectarea pentru distrugere a materialelor cu termenele de păstrare expirate se face de către comisia de experţi, care a efectuat expertiza valorii acestora. Materialele selectate pentru distrugere se includ într-un proces-verbal, conform formei nr. 47, anexă la prezentul Regulament, care va fi semnat de membrii comisiei de experţi şi aprobat de conducătorul instituţiei.

440. Materialele secretizate cu parafa „Strict secret", altele decît cele menţionate în punctul 439 din prezentul Regulament luate în evidenţă, se distrug în prezenţa şefului Subdiviziunii de protecţie şi a unei persoane autorizate să aibă acces la astfel de informaţii, în baza unui proces-verbal întocmit conform formei nr. 47, anexă la prezentul Regulament, aprobat de conducătorul autorităţii publice sau al altei persoane juridice. Procesul-verbal de distrugere este semnat de către şeful Subdiviziunii de protecţie şi de persoana care asistă la distrugere.

441. Distrugerea materialelor avînd gradele de secretizare „Secret", „Confidenţial" şi „Restricţionat", altele decît cele menţionate în punctul 439 din prezentul Regulament, luate în evidenţă, se face în baza unui proces-verbal întocmit conform formei nr. 47, anexă la prezentul Regulament, în prezenţa a două persoane care dispun de dreptul de acces la secretul de stat de forma respectivă, dintre care cel puţin una este din cadrul Subdiviziunii de protecţie. Procesul-verbal este semnat de către persoanele care asistă la distrugere, avizat de Subdiviziunea de protecţie şi aprobat de conducătorul autorităţii publice sau

al altei persoane juridice.

442. După finisarea verificării anuale a disponibilului de documente, fişele de evidenţă provizorie de asemenea se distrug, fapt ce va fi consemnat într-un proces-verbal.

443. Documentele de lucru, ciornele sau materialele acumulate sau create în procesul de elaborare a unui document, care conţin informaţii atribuite la secret de stat, de regulă, se distrug. În cazul în care se păstrează, acestea vor fi datate, parafate conform gradului cel mai înalt de secretizare a informaţiilor conţinute, arhivate şi protejate corespunzător gradului de secretizare a documentului final.

444. Distrugerea ciornelor documentelor ce conţin informaţii atribuite la secret de stat se realizează de către persoanele care le-au elaborat, în comun cu un angajat al Subdiviziunii de protecţie. Procesul-verbal de distrugere a ciornelor se întocmeşte în cazul în care acestea au fost înregistrate într-o formă de evidenţă.

445. În situaţii de urgenţă, protecţia, inclusiv prin distrugere, a materialelor secretizate cu parafa „Strict secret" are întotdeauna prioritate faţă de alte materiale.

446. Dacă din dosarele supuse distrugerii se extrag anumite documente necesare activităţii ulterioare, în procesul-verbal se indică tipul documentelor şi din care dosare sînt extrase (numărul de înregistrare, denumirea documentelor, numerele dosarelor şi filelor), precum şi în care dosare noi, după care numere de file sînt cusute documentele extrase sau înregistrate în registrele anului în curs.

447. În registrele de evidenţă se fac însemnările privind locul aflării documentelor extrase, iar în procesul-verbal de distrugere se indică numărul real al filelor rămase la dosarul ce urmează a fi distrus.

448. Dosarele se distrug împreună cu inventarul interior, după verificarea obligatorie a fiecărei file, cu înscrierile respective în actele şi inventarele interioare ale dosarelor.

449. Denumirea, numărul de înregistrare, numărul exemplarului, parafa de secretizare, numărul de exemplare şi de file ale fiecărui document (material) care urmează a fi distrus se verifică pînă la includerea acestuia în procesul-verbal, conform registrelor de evidenţă.

450. Materialele selectate şi incluse în procesul-verbal de distrugere se păstrează separat de alte materiale, în ambalaj sigilat.

451. Operarea unor rectificări în procesele-verbale de distrugere nu se admite. În cazuri excepţionale, operarea rectificărilor se va certifica prin semnăturile tuturor celor care au semnat procesul-verbal.

452. Se interzice distrugerea materialelor pînă la aprobarea procesului-verbal în modul stabilit.

453. Pînă la distrugere, se verifică corespunderea materialelor cu informaţia indicată în procesul-verbal.

454. Distrugerea materialelor trebuie să se efectueze în cel mai scurt termen posibil, după aprobarea procesului-verbal. Dacă materialele destinate distrugerii sînt transportate în afara autorităţii publice sau al altei persoane juridice, atunci ele se distrug în aceeaşi zi.

455. Transportarea materialelor la locul de distrugere se efectuează în ambalaj sigilat.

456. Materialele se distrug de către persoanele care au participat la verificarea acestora şi au semnat procesul-verbal de distrugere.

457. După distrugerea materialelor, în procesul-verbal se fac înscrierile respective cu privire la acest fapt, iar în registrele de evidenţă se va indica numărul procesului-verbal de distrugere şi data înregistrării lui.

458. Se interzice operarea modificărilor în procesul-verbal de distrugere după verificarea materialelor, efectuarea înscrierilor în registrele de evidenţă pînă la distrugerea materialelor sau transportarea proceselor-verbale, inventarelor sau altor documente, care nu sînt destinate distrugerii, la locul de distrugere a materialelor.

459. Procesele-verbale de distrugere se clasează şi se păstrează în dosare speciale ale Subdiviziunii de protecţie.

460. Procesele-verbale de distrugere a dosarelor se păstrează permanent, iar procesele-verbale de distrugere a altor materiale – timp de 10 ani.

Secţiunea a 11-a

Controlul disponibilului de documente secrete

461. Subdiviziunea de protecţie, cel puţin o dată în trimestru, verifică disponibilul tuturor documentelor primite, luate în evidenţă în perioada de control, care nu sînt clasate în dosare sau nu sînt completate în mape separate.

462. Anual, pînă la data de 1 martie, se verifică disponibilul tuturor documentelor şi dosarelor avînd gradele de secretizare „Strict secret", „Secret", „Confidenţial" şi „Restricţionat", indiferent de timpul primirii sau întocmirii lor şi de faptul unde şi la cine se află, cu excepţia arhivelor.

463. Controlul se efectuează de către o comisie specială, instituită prin ordinul (decizia) conducătorului autorităţii publice sau al altei persoane juridice, formată din cel puţin trei persoane, care au atribuţie directă la documentele verificate şi acces la secretul de stat de forma respectivă, cu includerea obligatorie în componenţa ei a angajaţilor din Subdiviziunea de protecţie.

464. În cazul existenţei unui număr neînsemnat de documente atribuite la secret de stat, controlul poate fi efectuat de către conducătorul sau unul din

angajaţii autorităţii publice sau altei persoane juridice, în comun cu un angajat al Subdiviziunii de protecţie.

465. În timpul controlului se verifică circulaţia (primirea, transmiterea, multiplicarea, distrugerea) documentelor atribuite la secret de stat din anul supus verificării, efectuîndu-se concomitent confruntarea datelor de evidenţă cu documentele efectiv disponibile. În acest scop, se utilizează registre de evidenţă a documentelor, recipise, inventare, procese-verbale de distrugere a documentelor şi alte forme de evidenţă, inclusiv cele în care se înregistrează multiplicarea documentelor.

466. Rezultatele controlului se înscriu într-un proces-verbal în care se indică:

1) tipul controlului efectuat;

2) denumirea subdiviziunii în care s-a efectuat controlul;

3) temeiul efectuării controlului;

4) componenţa comisiei de control;

5) termenele efectuării controlului;

6) caracterizarea succintă a situaţiei lucrărilor de secretariat secrete şi asigurarea regimului secret în activitatea executanţilor cu documentele secrete;

7) numărul total de documente luate în evidenţă în perioada de control, separat, pe toate tipurile de evidenţă;

8) numărul şi denumirea documentelor care nu sînt luate în evidenţă, la cine au fost depistate şi din care motive nu au fost luate în evidenţă;

9) numărul documentelor şi numărul de evidenţă a documentelor care nu au fost prezentate în timpul verificării, pe numele cui au fost trecute şi motivele neprezentării lor;

10) încălcările cerinţelor prezentului Regulament admise de către angajaţii Subdiviziunilor de protecţie, de alţi angajaţi cu indicarea faptelor concrete, a numelui, prenumelui şi funcţiei celor care le-au comis;

11) deciziile şi propunerile privind rezultatele controlului şi măsurile de lichidare a încălcărilor depistate.

467. Procesul-verbal privind controlul efectuat este semnat de către membrii comisiei şi aprobat de conducătorul autorităţii publice sau al altei persoane juridice ori de către locţiitorul acestuia.

468. Despre rezultatele controlului asupra disponibilului documentelor secrete se fac menţiunile respective în inventarul interior al documentelor care se află la executant, în prezenţa acestuia.

469. Dacă în timpul controlului se constată lipsa unor documente secrete,

comisia va informa imediat despre acest fapt conducătorul autorităţii publice sau al altei persoane juridice, precum şi şeful Subdiviziunii de protecţie, care, la rîndul lor, vor asigura informarea autorităţilor publice cu împuterniciri de dispoziţie asupra informaţiilor respective şi a Serviciului de Informaţii şi Securitate.

470. Subdiviziunea de protecţie, cel puţin o dată în trimestru, verifică respectarea modului de asigurare a regimului secret de către executanţi la locul de muncă. Controlul se efectuează în prezenţa executanţilor, iar în cazurile în care aceştia lipsesc – în prezenţa şefului subdiviziunii interioare sau a locţiitorului acestuia.

471. Rezultatele controlului, încălcările depistate şi măsurile întreprinse pentru înlăturarea acestora sînt înscrise într-un registru special pentru evidenţa controalelor la locurile de muncă ale executanţilor, ţinut de Subdiviziunea de protecţie.

472. Executanţii vizaţi sînt informaţi, contra semnătură, despre înscrierile cu privire la control efectuate în registru.

473. Conducătorii autorităţilor publice şi ai altor persoane juridice, Subdiviziunile de protecţie, precum şi şefii subdiviziunilor interioare sînt obligaţi să întreprindă măsuri de înlăturare a tuturor încălcărilor depistate în urma controalelor şi să asigure, în limita competenţelor, respectarea regimului secret, în conformitate cu prevederile Legii şi ale prezentului Regulament.

Secţiunea a 12-a

Evacuarea documentelor secrete în situaţii de urgenţă

474. În situaţiile de urgenţă, sarcina principală a Subdiviziunii de protecţie a autorităţii publice sau a altei persoane juridice este de a asigura regimul secret în lucrul cu documentele secrete în locurile de evacuare şi la obiectivele neevacuate, conform cerinţelor prezentului Regulament şi planurilor de evacuare.

475. Subdiviziunea de protecţie trebuie să fie pregătită permanent pentru desfăşurarea activităţii în condiţiile unor situaţii de urgenţă. Fiecare persoană din cadrul Subdiviziunii de protecţie trebuie să-şi cunoască obligaţiile şi succesiunea acţiunilor, în caz de situaţii de urgenţă.

476. În vederea pregătirii pentru situaţii de urgenţă, Subdiviziunea de protecţie, în comun cu alţi specialişti din cadrul autorităţii publice sau ai altei persoane juridice, elaborează şi înaintează spre aprobare ai conducătorului acesteia documentele prin care se determină:

1) nomenclatorul documentelor şi dosarelor secrete, care urmează a fi transportate la locurile de evacuare, distruse sau predate în arhivă pentru păstrarea de stat, precum şi a celor care rămîn la faţa locului;

2) listele persoanelor responsabile pentru evidenţa şi păstrarea documentelor

şi dosarelor secrete, care urmează a fi evacuate şi paza acestora în momentul transportării, distrugerii sau predării la păstrare în arhiva de stat;

3) măsurile cu privire la paza documentelor şi dosarelor secrete în locurile de evacuare.

477. Toate documentele şi dosarele secrete se repartizează pe următoarele categorii, conform destinaţiei acestora:

1) categoria I – include documentele şi dosarele care se transportă la locurile de evacuare;

2) categoria a II-a – include documentele şi dosarele care urmează a fi distruse la faţa locului;

3) categoria a III-a – include documentele şi dosarele care se predau spre păstrare în Fondul Arhivistic al Republicii Moldova;

4) categoria a IV-a – include documentele şi dosarele care rămîn pe loc.

478. Repartizarea documentelor pe categorii se efectuează de către comisii special instituite, formate din şefi de subdiviziune (locţiitori ai acestora), angajaţi ai Subdiviziunii de protecţie. Repartizarea documentelor se aprobă de către conducătorii autorităţilor publice sau ai altor persoane juridice respective.

479. În locurile de păstrare a acestor documente şi dosare (safeuri, containere, dulapuri de metal, saci, serviete, alţi suporţi speciali) trebuie să fie afişate inscripţii cu privire la destinaţia documentelor şi dosarelor, precum şi numele, prenumele, funcţia persoanelor responsabile pentru evidenţa şi păstrarea lor.

480. Pentru transportare se selectează documentele şi dosarele secrete necesare în activitatea zilnică în locurile de evacuare.

481. Distrugerea documentelor şi dosarelor secrete se efectuează în condiţiile stabilite de prezentul Regulament, după adoptarea deciziei cu privire la evacuarea autorităţii publice sau al altei persoane juridice.

482. Predarea documentelor şi dosarelor secrete selectate pentru păstrarea de stat se efectuează în modul stabilit de prezentul Regulament. Locurile de predare a documentelor şi dosarelor de arhivă se determină din timp de către autorităţile publice sau a altei persoane juridice.

483. La obiectivul (sau o parte a acestuia) care nu se evacuează se păstrează numai documentele necesare activităţii curente, într-un număr strict limitat.

484. În timpul situaţiei de urgenţă, autorităţile publice sau alte persoane juridice vor asigura respectarea regimului secret stabilit.

485. În zona de evacuare, la indicaţia conducătorului autorităţii publice sau al altei persoane juridice care se evacuează, se stabileşte regimul secret, în conformitate cu cerinţele prezentului Regulament.

486. Odată cu apariţia situaţiei de urgenţă se intensifică controlul asupra disponibilului documentelor şi dosarelor secrete la locul de evacuare şi la obiectivul evacuat. Despre rezultatele controalelor efectuate este informat şeful Subdiviziunii de protecţie. Verificarea completă a documentelor şi dosarelor se efectuează imediat după încheierea evacuării.

487. În autorităţile publice sau alte persoane juridice, amplasate în zona de frontieră, arhive secrete nu se creează. Documentele şi dosarele secrete ce prezintă valoare istorică sînt transmise pentru păstrare în arhivele departamentale sau în alte locuri de către autorităţile publice sau alte persoane juridice în cauză, la indicaţia acestora.

488. Documentele şi dosarele secrete ale autorităţilor publice sau ale altor persoane juridice din zona de frontieră se repartizează în două categorii:

1) categoria I, include documentele şi dosarele care se transportă la locurile de evacuare;

2) categoria a II-a, include documentele care urmează a fi distruse la faţa locului.

489. La evacuare, documentele şi dosarele secrete din categoria I trebuie să fie împachetate în ambalaje speciale care, la iniţiativa Subdiviziunii de protecţie, se pregătesc din timp, într-un număr suficient. Transportarea acestor documente şi materiale se efectuează cu mijloace de transport acoperite, iar ordinea de transportare a acestora se stabileşte de către şeful Subdiviziunii de protecţie.

490. Pentru organizarea transportării şi sigilării ambalajului în care se află documentele şi dosarele secrete, conducătorul autorităţii publice sau al altei persoane juridice numeşte din timp o persoană responsabilă din cadrul Subdiviziunii de protecţie.

491. Transportarea se efectuează în conformitate cu prevederile prezentului Regulament.

492. Pentru amplasarea Subdiviziunii de protecţie, la locul de evacuare trebuie să fie destinate încăperi (spaţii) aparte, asigurate cu pază.

493. La locul de evacuare, documentele şi dosarele secrete se păstrează în cadrul Subdiviziunii de protecţie numai în dulapuri de metal sau containere speciale. În afara programului de muncă, executanţii sînt obligaţi să predea documentele secrete Subdiviziunii de protecţie pentru păstrare în ambalaj sigilat (spre exemplu, mape de lucru, serviete).

494. Se interzice de a scoate documentele secrete din zona de evacuare fără paza corespunzătoare.

495. În locurile de evacuare, lucrările de secretariat secrete se ţin în conformitate cu cerinţele stabilite de prezentul Regulament.

496. Pentru a asigura eliberarea la timp a documentelor şi dosarelor secrete, selectate şi pregătite în prealabil, necesare activităţii în timpul situaţiilor de urgenţă, se permite păstrarea acestora în mape de lucru (serviete, valize, containere) separate şi sigilate de către executanţi. Pentru aceste documente se întocmeşte un inventar în două exemplare, unul dintre care se predă contra semnătură (recipisă) responsabilului desemnat pentru organizarea transportării, iar al doilea se păstrează în mapa executantului.

497. Executanţii care pleacă la locul evacuării predau cheile de la safeurile personale Subdiviziunii de protecţie. Încăperile în care se află documentele şi dosarele secrete ce rămîn pe loc se asigură cu pază corespunzătoare.

498. După evacuarea obiectivului sau a unei părţi a acestuia, Subdiviziunea de protecţie va asigura verificarea încăperilor, depozitelor, safeurilor, fapt consemnat într-un proces-verbal.

499. Documentele şi dosarele secrete din categoria a II-a se distrug pe loc, despre care fapt se întocmeşte un proces-verbal, potrivit cerinţelor prezentului Regulament.

500. În caz de infectare a documentelor şi dosarelor care urmează a fi transportate (categoria I) cu substanţe radioactive, otrăvitoare, alte substanţe, se efectuează dezinfectarea (dezactivarea, degazarea) acestora. Dacă asemenea posibilităţi nu există, documentele şi dosarele respective se transportă, cu respectarea tuturor măsurilor de precauţie, în locuri sigure pentru dezinfectare.

501. În cazul unor pericole eminente de atac (acaparare), se efectuează distrugerea imediată sau evacuarea tuturor documentelor şi a dosarelor secrete.

Capitolul IV

REGULI SPECIFICE DE OPERARE CU DOCUMENTAŢIA TEHNICĂ SECRETĂ

Secţiunea 1

Cerinţe generale

502. Organizarea evidenţei, păstrării şi utilizării documentaţiei tehnice secrete se pune în sarcina subdiviziunilor de protecţie ale autorităţilor publice şi ale altor persoane juridice.

503. În autorităţile publice şi alte persoane juridice în care există un volum mare de documentaţie tehnică se creează subdiviziuni ale documentaţiei tehnice secrete, ce activează sub controlul Subdiviziunii de protecţie.

504. Pentru păstrarea documentaţiei tehnice şi pentru lucrul cu o astfel de documentaţie, sînt destinate încăperi speciale, care să asigure protecţia corespunzătoare a informaţiilor atribuite la secret de stat.

Secţiunea a 2-a

Evidenţa preliminară a documentaţiei tehnice secrete

505. Toate filele destinate pentru elaborarea manuscriselor şi originalelor documentaţiei tehnice secrete se înregistrează de către executanţi în subdiviziunile documentaţiei tehnice secrete, iar dacă acestea lipsesc – în Subdiviziunea de protecţie.

506. Înregistrarea filelor destinate pentru executarea manuscriselor şi a originalelor se efectuează în Registrul de evidenţă preliminară a documentaţiei tehnice secrete sau Fişa de evidenţă preliminară a documentaţiei tehnice secrete, potrivit formelor nr. 48 şi nr. 49, anexă la prezentul Regulament. Filele destinate pentru executarea documentaţiei tehnice secrete care au diferite denumiri şi/sau grade de secretizare se iau în evidenţă preliminară cu numere de înregistrare diferite.

507. Filele suplimentare necesare în procesul executării documentaţiei tehnice secrete se înregistrează cu acelaşi număr de evidenţă preliminară, indicîndu-se noua dată de înregistrare şi numărul de file.

508. Pe recto primei file se indică denumirea documentaţiei tehnice secrete elaborate.

509. Parafa de secretizare se aplică pe fiecare pagină a documentaţiei tehnice secrete, în colţul drept de sus, iar fiecare pagină se numerotează.

510. Pe fiecare filă luată în evidenţă se aplică ştampila de înregistrare, indicîndu-se numărul şi data, iar pe prima pagină se va indica numărul total de file.

511. Pe filele de formatul A0 şi A1, B0 şi B1, ştampila de înregistrare se aplică suplimentar pe recto în două colţuri pe diagonală.

512. Pe filele lipite (prinse), ştampila de înregistrare se aplică în locul în care acestea sînt lipite (prinse), iar în registrul de evidenţă se indică numărul acestora.

513. Pe filele broşate, ştampila de înregistrare se aplică pe copertă şi pe prima filă.

514. Aplicarea unor etichete pe filele luate în evidenţă preliminară se efectuează numai cu permisiunea Subdiviziunii de protecţie sau a subdiviziunilor documentaţiei tehnice secrete, despre care fapt, pe documente, se efectuează o însemnare legalizată.

515. După elaborarea manuscrisului documentaţiei tehnice secrete se pregăteşte originalul acesteia. Lista persoanelor care sînt în drept să permită executarea originalului după manuscris se aprobă de conducătorul autorităţii publice sau al altei persoane juridice.

516. Executarea originalului prin copiere manuală se efectuează pe file

luate în evidenţă preliminară, indicîndu-se pe ele parafa de secretizare, numărul exemplarului, denumirea şi marcarea documentului.

517. În cazul fotocopierii originalului, ştampila şi numărul de înregistrare se va asigura prin reproducerea de pe manuscris.

518. Semnele de înregistrare şi ştampilele se aplică în locurile stabilite de standardele respective.

519. După executarea originalului şi înregistrarea acestuia în registrul de evidenţă, manuscrisul documentaţiei tehnice secrete se distruge în modul stabilit de prezentul Regulament.

520. Executarea copiilor documentaţiei tehnice secrete, care se află în evidenţă preliminară, se efectuează ca excepţie, pentru prezentarea acesteia spre coordonare preventivă.

521. În cazul în care drept bază pentru elaborarea manuscrisului documentaţiei tehnice secrete este necesar a se utiliza copia documentaţiei tehnice secrete elaborate anterior, care se află în evidenţă preliminară sau de inventar, atunci această copie se radiază din evidenţa anterioară şi se înregistrează preliminar cu noua ei denumire.

522. Evidenţa preliminară poate fi asigurată în formă unică pentru toate tipurile de documentaţie tehnică secretă sau poate fi ţinută separat pentru diferite tipuri de documentaţie tehnică secretă, adăugîndu-se la numărul de evidenţă un indice distinctiv.

523. Evidenţa se ţine anual, începînd cu primul număr. Documentaţia tehnică secretă care urmează a fi transferată pe anul următor se înregistrează cu numere noi.

524. Registrele de evidenţă preliminară a documentaţiei tehnice secrete se păstrează în decurs de un an de la închiderea tuturor numerelor de evidenţă şi se distrug în baza unui proces-verbal.

525. Evidenţa fişelor de evidenţă a documentaţiei tehnice secrete se ţine în Registrul de evidenţă a circulaţiei fişelor, potrivit formei nr. 50, anexă la prezentul Regulament.

526. Fişele de evidenţă preliminară a documentaţiei tehnice secrete se ţin neîntrerupt. Fişele epuizate după verificarea anuală se distrug în baza unui proces-verbal, făcîndu-se însemnările respective în Registrul de înregistrare şi de evidenţă a circulaţiei fişelor.

Secţiunea a 3-a

Evidenţa de inventar a documentaţiei tehnice secrete

527. Se supune evidenţei de inventar:

1) documentaţia tehnică secretă, elaborată de autoritatea publică sau altă persoană juridică şi aprobată în modul stabilit;

2) documentaţia tehnică secretă, aprobată în modul stabilit, primită de la alte autorităţi publice sau persoane juridice, după înregistrarea acesteia în Registrul de control al plicurilor.

528. Nu se supune evidenţei de inventar documentaţia tehnică secretă care se clasează (coase) în dosar şi documentaţia tehnică secretă care a fost primită pentru coordonare sau pentru utilizare provizorie.

529. Evidenţa de inventar poate fi ţinută separat, conform diferitor criterii de clasificare (spre exemplu: denumire, tipul documentaţiei, tipul de executare).

530. Evidenţa de inventar se ţine conform formelor nr. 51, nr. 52 şi nr. 46, anexă la prezentul Regulament. Fişele evidenţei de inventar a documentaţiei tehnice secrete se ţin în evidenţă conform Registrului de înregistrare şi de evidenţă a circulaţiei fişelor.

531. Copiile documentaţiei tehnice secrete executate în autorităţile publice sau alte persoane juridice şi expediate destinatarilor se ţin în evidenţă în Fişele evidenţei de inventar a copiilor documentaţiei tehnice secrete (forma nr. 53, anexă la prezentul Regulament). Despre întocmirea acestor fişe se face o însemnare în Registrul evidenţei de inventar a documentaţiei tehnice secrete/Fişa evidenţei de inventar a documentaţiei tehnice secrete.

532. Autorităţile publice sau alte persoane juridice, care nu elaborează documentaţie tehnică secretă şi nu dispun de originale şi duplicate, pot ţine evidenţa copiilor, precum şi a ediţiilor secrete în Registrul evidenţei de inventar a materialelor scrise broşate.

533. Documentaţiei tehnice secrete luate în evidenţă după radierea ei din evidenţa preliminară i se acordă un singur număr de inventar, indiferent de numărul de file pe care a fost editată şi numerele de evidenţă care au fost incluse în ea. În cazurile în care se ţine evidenţa diferitor tipuri de documentaţie tehnică secretă, la numerele de inventar se vor adăuga indici distinctivi.

534. După ce documentaţia tehnică secretă a fost luată în evidenţa de inventar, aceasta se radiază din evidenţa preliminară.

535. La radierea documentaţiei tehnice secrete din evidenţa preliminară, în Registrul de evidenţă preliminară a documentaţiei tehnice secrete /Fişa de evidenţă preliminară a documentaţiei tehnice secrete se introduce numărul de inventar acordat acesteia, iar în Registrele prevăzute în formele nr. 51, nr. 52 şi nr. 46, anexă la prezentul Regulament, se face însemnarea cu privire la numărul de evidenţă preliminară a acestei documentaţii.

536. Pe fiecare filă din document, în locul stabilit de standardele respective, se aplică ştampila, indicîndu-se numărul de inventar şi data cînd a fost luat în evidenţă.

537. Dacă copiile originalului documentaţiei tehnice secrete urmează a fi broşate, numărul de inventar se aplică suplimentar pe cîmpul primei pagini şi al foii de titlu (dacă există). Pe documentaţia tehnică secretă în formă textuală, numărul de inventar se aplică în partea de sus a primei pagini şi a foii de titlu, iar pe cele grafice – mai sus de înscrierea principală.

538. Pe documentaţia tehnică secretă recepţionată de la alte autorităţi publice sau persoane juridice, numărul de inventar şi datele luării în evidenţă se aplică:

1) pe originale – pe cîmpul de coasere a fiecărei file, iar numerele de înregistrare se vor trasa cu tuş în linii subţiri;

2) pe duplicate – în rubrica stabilită a fiecărei file;

3) pe documentele completate în mape sau broşate în albume – pe etichete sau în colţul stîng de sus al copertei, precum şi pe prima pagină sau foaie de titlu a inventarului şi pe foaia de titlu (dacă există) a mapei (albumului);

4) pe copiile ce se păstrează în file aparte – în colţul stîng de sus al fiecărei file.

539. Documentaţia tehnică secretă care se ţine în evidenţă de inventar poate fi eliberată executanţilor în caz de necesitate de serviciu.

540. Originalele documentaţiei tehnice secrete se eliberează pentru executarea copiilor şi duplicatelor, operarea în ele a modificărilor, precum şi pentru restabilirea lor. Originalele se eliberează executanţilor numai la indicaţia scrisă a şefului subdiviziunii interioare, iar originalele documentaţiei tehnice avînd gradul de secretizare „Strict secret" – la indicaţia scrisă a conducătorului autorităţii publice sau al altei persoane juridice.

Secţiunea a 4-a

Păstrarea documentaţiei tehnice secrete

541. Documentaţia tehnică secretă se păstrează conform regulilor stabilite în standardele de stat, respectîndu-se cerinţele prezentului Regulament.

542. Originalele documentaţiei tehnice secrete pot fi completate şi păstrate în mape.

543. Copiile documentaţiei tehnice secrete se păstrează şi se expediază altor autorităţi publice sau persoane juridice atît pe file aparte, cît şi completate în mape sau broşate în albume.

544. Documentaţia tehnică secretă se completează în mape (albume), în caz de necesităţi de producţie, respectîndu-se condiţiile cu privire la informarea executanţilor numai cu informaţia necesară lor.

545. Mapei sau albumului i se atribuie un număr nou de inventar, iar parafa de secretizare se aplică în conformitate cu gradul de secretizare a informaţiilor

cuprinse în documentaţia tehnică secretă din mapă (album).

546. În inventarul anexat la mapă (album) se enumeră, în ordine succesivă, documentaţia tehnică secretă conţinută în aceasta (denumirea documentelor, gradul de secretizare, numărul de evidenţă, numerele exemplarelor, numărul de file). Enumerarea filelor la întocmirea inventarului anexat la mapa (albumul) documentaţiei tehnice secrete se începe cu foaia de titlu.

547. Numărul de inventar al documentaţiei tehnice secrete incluse în mapă (album), se închide prin menţiunea „inclus în numărul de inventar ___”, înscrisă în registrele prevăzute în formele nr. 51, nr. 52 şi nr. 46, anexă la prezentul Regulament.

548. Copiile broşate ale documentaţiei tehnice secrete în formă textuală poartă numărul de inventar al originalului.

549. Fotoimprimările secrete anexate la copii se lipesc pe filele luate în evidenţă. Numărul acestora se confirmă prin semnătura legalizată şi se înscrie în registrele prevăzute în formele nr. 51 şi nr. 52, anexă la prezentul Regulament.

550. Se interzice aplicarea unor imprimări sau etichete care conţin informaţii atribuite la secret de stat pe coperta documentaţiei tehnice secrete.

551. Registrele evidenţei de inventar a documentaţiei tehnice secrete nu pot fi eliberate executanţilor.

552. Pentru căutarea documentaţiei tehnice secrete luate în evidenţa de inventar se întocmesc fişiere şi cataloage speciale, care pot fi ţinute atît în formă manuală, cît şi electronică, cu respectarea cerinţelor stabilite pentru asigurarea protecţiei secretului de stat.

Secţiunea a 5-a

Operarea modificărilor în documentaţia tehnică secretă

553. Operarea modificărilor în documentaţia tehnică secretă, precum şi anularea (abrogarea) ei se efectuează conform avizului cu privire la modificare şi regulilor expuse în standardele de stat corespunzătoare, respectîndu-se cerinţele prezentului Regulament.

554. Avizul cu privire la modificări se întocmeşte de autorităţile publice sau alte persoane juridice, deţinători ai originalelor. Avizele secrete cu privire la modificări se iau în evidenţa de inventar conform formelor nr. 51 şi nr. 52, anexă la prezentul Regulament.

555. Toate modificările în documentaţia tehnică secretă se operează de angajaţi special desemnaţi din subdiviziunile documentaţiei tehnice secrete din cadrul autorităţilor publice sau altor persoane juridice. În caz de necesitate, în această activitate pot fi antrenate persoane din cadrul subdiviziunilor interioare

de producţie, care au acces la documentaţia tehnică secretă supusă modificării.

556. Modificările se înregistrează în tabelul de modificări sau în lista de înregistrare a modificărilor. Dacă pe document nu există loc suficient pentru operarea modificărilor sau în timpul efectuării modificărilor poate fi afectată claritatea imaginii, se pregătesc file aparte ale originalului, cu luarea în calcul a modificărilor respective şi păstrîndu-se numărul de inventar precedent.

557. Dacă originalul documentaţiei tehnice secrete se înlocuieşte în întregime cu un alt original, acestuia din urmă i se acordă un nou număr de inventar. Această documentaţie tehnică secretă se înregistrează în registrele prevăzute în formele nr. 51 şi nr. 52, anexă la prezentul Regulament. Pe originalul anterior al documentaţiei tehnice secrete se face o menţiune despre înlocuirea lui, cu referire la numărul nou de inventar.

558. Dacă se înlocuiesc unele file din original, pe ele se păstrează numărul de inventar. Menţiunea cu privire la înlocuirea acestor file (fără modificarea numărului total de file) se înscrie în Registrul evidenţei de inventar a documentaţiei tehnice secrete/Fişa evidenţei de inventar a documentaţiei tehnice secrete. Totodată, modificarea numărului de file va fi reflectată şi în Fişa evidenţei de inventar a copiilor documentaţiei tehnice secrete.

559. Originalele (unele file) înlocuite ale documentaţiei tehnice secrete se păstrează de rînd cu originalele în vigoare.

560. Înlocuirea unor file ale copiilor documentaţiei tehnice secrete se efectuează prin rebroşare şi efectuarea unei noi înscrieri legalizate pe o filă separată, ataşată după fila cu înscrierea legalizată anterioară, care la fel rămîne în broşură. Noua înscriere poate fi făcută pe aceeaşi filă cu înscrierea anterioară, dacă există loc suficient. Filele înlocuite ale copiilor se distrug în modul stabilit, imediat după operarea modificărilor.

561. În documentaţia tehnică secretă editată prin metode tipografice, modificările se operează prin trasarea textului sau imaginilor grafice cu tuş. Dacă se modifică o parte a textului, atunci pe filele modificate se face o referinţă la suplimentele editate.

562. Pregătirea (restabilirea) originalelor documentaţiei tehnice secrete în locul celora care au devenit inutilizabile se efectuează numai după întocmirea procesului-verbal despre anularea lor.

563. Restabilirea originalelor se efectuează pe file luate în evidenţă preliminară. Originalele restabilite se iau în evidenţă sub aceleaşi numere de inventar prin efectuarea înscrierii respective în registrele prevăzute în formele nr.51 şi nr.52, anexă la prezentul Regulament. Pe originalul restabilit se aplică menţiunea „original restabilit nr. ___”, indicîndu-se numărul de ordine al procedurii de restabilire. Originalul care conţine cîteva file poate fi restabilit parţial, indicîndu-se acest fapt în registrele prevăzute în formele nr.51 şi nr.52,

anexă la prezentul Regulament. Pe fila de înregistrare a modificării originalului restabilit se reproduc datele cu privire la toate modificările operate anterior în acest document. Originalele anulate care au devenit inutilizabile se retrag din circulaţie şi se păstrează separat de cele în vigoare, în decurs de un an, iar apoi se distrug, fapt care se consemnează într-un proces-verbal.

564. Duplicatele nu se restabilesc. La necesitate, ele se execută repetat.

Capitolul V

REGULI PRIVIND EFECTUAREA LUCRĂRILOR SECRETE DE FILMARE ŞI FOTOGRAFIERE

Secţiunea 1

Lucrările de filmare şi fotografiere, evidenţa documentelor cinematografice şi fotografice secrete

565. Lucrările de filmare pentru producerea filmelor secrete se efectuează în cazurile în care există un scenariu (plan de scenariu), coordonat cu autorităţile publice interesate şi cu beneficiarul respectiv, aprobat de către conducătorul autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii.

566. Filmarea şi fotografierea unor procese secrete se efectuează în conformitate cu planurile de activitate ale autorităţilor publice şi ale altor persoane juridice, aprobate de conducerea autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii.

567. Accesul grupului de filmare (executantului) la filmări (fotografiere) se efectuează cu permisiunea în scris a conducătorului autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii, în care se indică lista obiectelor (proceselor) care urmează a fi filmate (fotografiate), componenţa grupului de filmare şi termenul de îndeplinire a lucrărilor.

568. Gradul de secretizare a filmului în întregime, a unor imagini, fonograme sincronice şi textului crainicului, a altor elemente ale acestuia se determină de către autoritatea publică sau altă persoană juridică – beneficiar, în timpul scrierii şi coordonării scenariului (planului de scenariu), în conformitate cu prevederile prezentului Regulament.

569. Este interzisă filmarea, fotografierea şi prezentarea video a proceselor de fabricare şi testare a articolelor avînd gradul de secretizare „Strict secret”. În caz de necesitate, aceste acţiuni pot fi efectuate doar cu permisiunea conducătorilor autorităţilor publice cu împuterniciri de dispoziţie asupra informaţiilor respective şi a beneficiarului, în prezenţa şefului Subdiviziunii de protecţie a autorităţii publice sau al altei persoanei juridice unde se efectuează filmările, fotografierea sau prezentarea video.

570. Lucrările de filmare pentru producerea filmelor secrete pot fi efectuate de către autorităţile publice, precum şi în studiourile şi laboratoarele cinemato-

grafice ale persoanelor juridice care dispun de certificatul de securitate respectiv.

571. Numărul persoanelor care participă nemijlocit la procesul de filmare şi creare a documentelor cinematografice şi fotografice trebuie să fie cît mai limitat. Componenţa grupurilor de filmare şi autorii scenariilor secrete (planurilor de scenariu) se aprobă de către autoritatea publică cu împuterniciri de dispoziţie asupra informaţiilor respective. Responsabil pentru filmare este o persoană din cadrul Subdiviziunii de protecţie.

572. Filmarea şi fotografierea informaţiilor secrete, prelucrarea materialului filmat, executarea, copierea filmelor secrete se efectuează în conformitate cu Foaia de comandă privind executarea lucrărilor fotografice secrete (forma nr. 54, anexă la prezentul Regulament) cu utilizarea materialelor cinematografice şi fotografice marcate şi luate în evidenţă de Subdiviziunea de protecţie, pînă la începerea acestor lucrări. Numerele de inventar ale materialelor cinematografice şi fotografice se indică în foile de comandă privind executarea lucrărilor fotografice secrete.

573. Evidenţa de inventar a negativelor fotografice, a pozitivelor (imprimărilor foto), a diapozitivelor imprimate de pe ele, a suporţilor electronici se ţine în Registrul de evidenţă a negativelor fotografice şi fotoimprimărilor (forma nr. 55, anexă la prezentul Regulament). În acest registru se ţin în evidenţă şi negativele fotografice, imprimările fotografice şi diapozitivele, suporţii electronici primiţi de la alte autorităţi publice sau alte persoane juridice.

574. Documentele cinematografice şi fotografice (negativele, pozitivele, diapozitivele, suporţii electronici) cu aceeaşi denumire, grad de secretizare al unuia şi aceluiaşi obiect se iau în evidenţă în Registrul de evidenţă a negativelor fotografice şi fotoimprimărilor cu acelaşi număr de inventar, indicîndu-se numărul exemplarului.

575. În cazurile în care nu există posibilitatea de a marca capetele peliculei, aparatul de filmare sau de fotografiere încărcat cu o atare peliculă trebuie să fie sigilat. Descărcarea şi încărcarea aparatelor de filmat şi de fotografiat sigilate în procesul filmării (fotografierii) se efectuează în prezenţa unei persoane din cadrul Subdiviziunii de protecţie. Caseta filmată se plasează într-o cutie specială, care se sigilează. Dacă nu există posibilitatea de a marca pelicula şi placa fotografică, ele se eliberează la unitate şi de fiecare format aparte. Informaţia de pe suportul electronic se transferă, în prezenţa unei persoane din cadrul Subdiviziunii de protecţie, pe un alt tip de suport, cu întocmirea unui proces-verbal în conformitate cu prezentul Regulament. Suportul de informaţie se plasează într-o cutie specială, care se păstrează în conformitate cu prezentul Regulament. Informaţia iniţială după copiere se nimiceşte prin formatarea dispozitivului de fotografiere sau filmare folosit.

576. Se interzice de a diviza (fragmenta) peliculele cinematografice şi materialele fotografice cu capetele marcate, pregătite pentru filmare. Dacă

în timpul filmărilor secrete s-au produs rupturi ale peliculelor, acest fapt se consemnează în procese-verbale corespunzătoare.

577. Peliculele uzate se expun iluminării şi se distrug, fapt ce se reflectă în Registrul de evidenţă a negativelor fotografice şi fotoimprimărilor.

578. Filmelor cinematografice secrete şi altor documente cinematografice secrete, în caz de necesitate, li se atribuie denumiri convenţionale. Filmarea, prelucrarea, sonorizarea, copierea, montarea şi tirajarea documentelor cinematografice secrete se înregistrează în registrele de evidenţă, elaborate de subdiviziunile de protecţie, ţinîndu-se cont de cerinţele prezentului Regulament.

579. Pe fiecare negativ developat, căruia i s-a atribuit un număr de evidenţă, executantul lucrării indică parafa de secretizare, numărul de evidenţă, data, numărul exemplarului, metrajul peliculei, numărul cadrelor, numele şi prenumele său. În cazul suporţilor electronici, se va indica capacitatea acestora.

580. Dacă din cauza dimensiunii mici a peliculei este imposibil de a face aceste înscrieri pe negativ, pînă la începerea filmării, ele se efectuează pe şabloane speciale, care se fixează în partea dreaptă, mai sus de obiectul filmării şi împreună cu acestea se fotografiază.

581. În cazul în care nu este posibil de a fixa şablonul pe obiectul de filmare, acesta se fotografiază la începutul şi sfîrşitul filmării. În cazul filmării mai multor teme pe una şi aceeaşi peliculă, şabloanele se filmează înainte şi la finalizarea fiecărei teme. Parafa de secretizare se indică pe cadrul de titlu al filmului şi la începutul textului crainicului. Pe fotografii, parafa de secretizare se aplică pe recto documentelor fotografice.

582. Negativele cinematografice şi fotografice, peliculele fotografice, suporţii electronici se păstrează în dulapuri de metal, separate de alte documente. Pe capacul cutiilor de metal se indică: parafa de secretizare, denumirea convenţională, numărul rolei (bobinei), numărul de evidenţă al acesteia, desenul şi numărul lipiturilor.

583. Cînd există un număr mare de negative cinematografice şi pelicule fotografice, ele se păstrează în încăperi speciale dotate cu mijloace de protecţie împotriva incendiilor. După dispariţia necesităţii practice şi după expirarea termenului de păstrare, negativele şi fotografiile se distrug în baza unui proces-verbal, cu reflectarea acestui fapt în Registrul de evidenţă a negativelor fotografice şi fotoimprimărilor.

584. Fotografiile montate în alte documente secrete se radiază din Registrul de evidenţă a negativelor fotografice şi fotoimprimărilor, în care se înscriu numerele de inventar şi numerele exemplarelor documentelor la care acestea se anexează.

585. În ambalajul în care materialele secrete (cinematografice şi fotografice) filmate se prezintă studioului cinematografic (laboratorului cinematografic şi

fotografic) sau beneficiarului filmului pentru a fi prelucrate, se plasează un inventar în care se indică: parafa de secretizare, denumirea convenţională a documentelor cinematografice şi fotografice şi numărul bobinelor. Persoana din cadrul studioului (laboratorului) cinematografic este obligată să controleze integritatea ştampilelor la primirea materialelor în Subdiviziunea de protecţie, iar după developarea peliculei – marcarea şi integritatea ei. Se interzice prelucrarea materialelor cinematografice şi fotografice secrete care nu au fost luate în evidenţă în modul stabilit.

586. Dacă filmul cinematografic conţine cîteva părţi, pe fiecare parte a acestuia trebuie să existe racorduri standard, pe care se indică: parafa de secretizare, metrajul (volumul), numărul lipiturilor, numărul părţii (bobinei), tema, comanda şi numărul de inventar.

587. Fiecare parte se plasează într-o cutie de metal aparte, pe care se înscriu toate datele menţionate în racorduri.

588. Cadrele rebutate, precum şi cadrele neprevăzute în comandă (scenariu) se retrag (se decupează) şi se distrug, în modul stabilit. La fel se retrag şi se distrug şi resturile (fragmentele) peliculei în procesul montării filmului.

589. Filmul cinematografic finisat este recepţionat de o comisie, în componenţa căreia se includ reprezentanţi ai autorităţilor publice interesate şi ai beneficiarului.

590. Comisia întocmeşte un proces-verbal în care se va consemna faptul dacă filmul cinematografic corespunde scenariului aprobat (planului de scenariu), parafei de secretizare, va menţiona metrajul (volumul) şi alte date necesare. Procesul-verbal se aprobă de persoana care a aprobat scenariul (planul de scenariu) şi va servi drept bază pentru ca filmul cinematografic să fie luat în evidenţa de inventar.

591. Multiplicarea filmelor cinematografice secrete şi transmiterea lor se efectuează într-un număr strict limitat, determinat de conducerea autorităţii publice care a aprobat scenariul cinematografic. Se interzice efectuarea fotografiilor de pe cadrele cinematografice. În caz de necesitate, de pe anumite cadre, cu permisiunea conducătorului autorităţii publice cu împuterniciri de dispoziţie asupra informaţiilor respective, de comun cu beneficiarul, pot fi executate fotografii sau diapozitive, care sînt luate în evidenţa de inventar ca documente cinematografice şi fotografice separate.

592. Aparatele de filmat şi de fotografiat pentru filmări secrete se iau în evidenţă şi se păstrează în laboratoarele cinematografice şi fotografice şi se eliberează contra recipisă în registrul de evidenţă.

593. Scenariile (planurile de scenariu), planurile de filmare, sarcinile şi alte documente ce se referă la lucrările cinematografice şi fotografice se clasează în dosare separate.

594. Eliberarea copiilor de pe documentele cinematografice secrete pentru o singură vizionare se efectuează cu permisiunea în scris a conducătorului autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii şi avizul Subdiviziunii de protecţie. Copiile documentelor cinematografice avînd gradul de secretizare „Secret", „Confidenţial" şi „Restricţionat" pot fi eliberate cu permisiunea în scris a locţiitorului conducătorului autorităţii publice responsabil de asigurarea regimului secret sau cu permisiunea scrisă a şefului Subdiviziunii de protecţie.

595. Transmiterea filmelor cinematografice secrete se face prin intermediul Serviciului de Stat de Curieri Speciali. Filmul cinematografic se prezintă împreună cu paşaportul tehnic al acestuia, care se restituie împreună cu filmul.

596. Demonstrarea filmelor cinematografice secrete se efectuează cu respectarea cerinţelor stabilite pentru şedinţele secrete.

597. Se interzice începerea demonstrării filmelor cinematografice secrete în lipsa persoanei desemnate responsabilă pentru vizionare. Vizionarea filmelor cinematografice secrete se înregistrează de Subdiviziunea de protecţie într-un registru special în care se indică data, denumirea filmului cinematografic sau tema, parafa de secretizare, scopul demonstrării, timpul (ora) prezentării, numele, prenumele persoanei responsabile pentru vizionare şi ale persoanei care demonstrează filmul.

598. În toate cazurile de demonstrare a filmelor cinematografice secrete se întreprind măsuri care ar exclude pierderea sau extinderea informaţiei în afara zonei controlate.

599. Modificarea metrajului filmului secret şi a numărului de lipituri în cazurile în care se rupe pelicula cinematografică în timpul demonstrării filmului se consemnează într-un proces-verbal şi se reflectă în paşaportul tehnic al filmului cinematografic, indicîndu-se temeiul operării modificărilor. Procesul-verbal se semnează de persoana responsabilă pentru demonstrarea filmului cinematografic şi se aprobă de şeful Subdiviziunii de protecţie.

Secţiunea a 2-a

Microfilmarea, evidenţa şi păstrarea microfilmelor

600. Documentele secrete pot fi microfilmate sau stocate pe discuri optice ori pe suporţi magnetici în următoarele condiţii:

1) procesul de microfilmare sau stocare să fie realizat cu aprobarea autorităţii cu împuterniciri de dispoziţie asupra informaţiei respective de către personalul care dispune de dreptul de acces la secretul de stat de forma corespunzătoare gradului de secretizare a informaţiilor respective;

2) pentru microfilmele, discurile optice sau suporţii magnetici de stocare să se asigure aceeaşi protecţie ca şi pentru documentul original;

3) toate microfilmele, discurile optice sau suporţii magnetici de stocare să fie înregistrate într-o evidenţă specifică şi supuse, ca şi documentele originale, verificării anuale.

601. Lucrările de microfilmare a documentelor secrete se efectuează prin intermediul Subdiviziunii de protecţie, în baza Foii de comandă privind executarea lucrărilor fotografice secrete. Foaia de comandă privind executarea lucrărilor fotografice secrete se eliberează după verificarea seturilor pregătite pentru microfilmare şi a stării documentelor recepţionate, precum şi după întocmirea schemei de formare a bobinelor.

602. Peliculele eliberate pentru microfilmarea documentelor secrete se compostează la ambele capete de către Subdiviziunea de protecţie, fapt ce se reflectă în Foaia de comandă privind executarea lucrărilor fotografice secrete.

603. Înainte de începerea lucrărilor de microfilmare, Subdiviziunea de protecţie va asigura sigilarea casetelor fotografice (camerelor) încărcate cu peliculă.

604. Evidenţa documentaţiei ce urmează a fi microfilmată de către laboratoarele de microfilmare (laboratoarele speciale) se ţine în Registrul de evidenţă a documentaţiei primite pentru microfilmare (forma nr. 56, anexă la prezentul Regulament). În caz de necesitate, fiecare unitate din set (dosar, document aparte) se înregistrează cu un număr aparte.

605. Microfilmul trebuie să conţină microimaginea deplină a setului cu originalele documentelor. În cazurile în care există un volum mic de documente, se permite plasarea cîtorva microfilme pe un singur purtător al microimaginilor (bobină, microfişă, alt purtător material).

606. La microfilmarea documentelor din cîteva cadre, fiecare cadru trebuie să conţină o parte din imaginea documentului inclus în cadrul precedent sau în cel ce urmează.

607. După încheierea filmării, casetele (camerele) cu pelicula sigilată se transmit sectorului (subdiviziunii) de developare a microfilmelor, împreună cu foaia de comandă, în aşa mod ca să fie asigurată evidenţa acestora. Originalul documentului se restituie Subdiviziunii de protecţie.

608. Microfilmul secretizat trebuie să conţină un cadru de control cu imaginea obiectului şi şablonului de identificare, care include:

1) parafa de secretizare;

2) genul microfilmului (de bază, de rezervă);

3) numărul de înregistrare a foii de comandă;

4) numărul de înregistrare a microfilmului;

5) marcarea microfilmului sau a unei părţi a acestuia;

6) deţinătorul originalului;

7) denumirea persoanei juridice care a efectuat microfilmarea;

8) felul documentaţiei;

9) denumirea sau semnul convenţional al art. (obiectului);

10) marcarea documentaţiei;

11) datele cu privire la numărul de file filmate în microfilm;

12) date cu privire la numărul de cadre în microfilm (fără a se lua în calcul şablonul);

13) proporţia micşorării imaginii;

14) data microfilmării.

609. Dacă microfilmul este alcătuit din cîteva bobine sau microfişe, atunci la sfîrşitul fiecărei bobine sau microfişe, cu excepţia ultimei, se aplică menţiunea „Va urma", iar la începutul fiecărei bobine, cu excepţia primei, se aplică menţiunea „Continuare".

610. În caz de necesitate, pe şablon se aplică menţiuni cu privire la modificări şi completări – „Imprimare suplimentară" sau „Modificare".

611. După şablon se microfilmează lista de însoţire a documentaţiei, iar ulterior – setul de documente indicat în lista respectivă. Şablonul se plasează la începutul şi la sfîrşitul microfilmului şi pe fiecare parte a acestuia.

612. Bobinele rebutate ale microfilmului sau ale unor cadre ale acestuia se distrug în baza unui proces-verbal.

613. Filmarea suplimentară a unor cadre aparte sau a bobinei în întregime pentru înlocuirea celor rebutate se efectuează cu acelaşi număr de înregistrare, atribuit microfilmului (bobinei) în această documentaţie, dar în baza unei noi foi de comandă.

614. Bobinele microfilmelor secrete finisate, după ce au fost luate în evidenţa de inventar şi după verificarea calităţii acestora, se pun în cutii de metal speciale, se sigilează şi se transmit, contra semnătură (recipisă), Subdiviziunii de protecţie. Pe capacul cutiei se aplică numărul atribuit microfilmului (bobinei), parafa de secretizare, forma imaginii, tipul microfilmului (de bază, de rezervă), metrajul şi numărul lipiturilor. Subdiviziunea de protecţie înregistrează microfilmul în Registrul de evidenţă a microfilmelor (forma nr. 57, anexă la prezentul Regulament) şi expediază cutia cu microfilm (bobină) persoanei care a făcut comanda pentru păstrare permanentă.

615. Păstrării se supun două tipuri de microfilme: de bază şi de rezervă. Microfilmul de bază este destinat pentru executarea copiilor documentelor, iar cel de rezervă – pentru restabilirea microfilmului de bază, în caz de deteriorare. Microfilmului de bază şi celui de

rezervă i se atribuie un singur număr şi aceeaşi marcare.

616. Bobina micropeliculei ce conţine microimaginile documentaţiei modificate se lipeşte de microfilmul produs anterior sau se păstrează separat. Toate modificările care se includ în microfilme sînt reflectate în documentele de evidenţă.

617. Microhărţile efectuate de pe microfilmele secrete se trec în evidenţă în Registrul de evidenţă a negativelor fotografice şi fotoimprimărilor. Pe fiecare filă a microhărţii în colţul drept de sus se indică: parafa de secretizare, numărul microfilmului, numărul exemplarului, numărul de inventar al filei, iar prin cratimă – numărul cadrelor în microhartă.

Capitolul VI

REGULI DE OPERARE CU ARTICOLE SECRETE

Secţiunea 1

Respectarea regimului secret la producerea articolelor secrete şi utilizarea lor

618. Asigurarea măsurilor privind respectarea regimului secret la proiectarea, producerea, păstrarea, transportarea şi exploatarea articolelor secrete se efectuează de către conducătorii autorităţilor publice şi ai altor persoane juridice, şefii subdiviziunilor respective, în colaborare cu Subdiviziunile de protecţie.

619. Articolelor şi părţilor lor componente li se pot atribui denumiri sau semne convenţionale, care nu trebuie să dezvăluie existenţa acestora, caracterul, destinaţia, particularităţile tehnice şi de alt gen. Denumirile convenţionale ale articolelor pot fi indicate, în caz de necesitate, numai în documentele secrete.

620. Expunerea la expoziţii a articolelor secrete, de regulă, nu se admite. În caz de necesitate, cu permisiunea autorităţilor publice cu împuterniciri de dispoziţie asupra acestor informaţii şi sub controlul Subdiviziunilor de protecţie respective, pot fi organizate expoziţii secrete speciale. Aceste expoziţii pot fi vizitate de către persoanele care au acces la secretul de stat de forma respectivă şi au atribuţie la articolele secrete expuse în cadrul expoziţiei.

621. Posibilitatea de expunere la expoziţie a noilor mostre de articole se coordonează cu beneficiarul.

622. Numărul de persoane care au dreptul să lucreze şi să ia cunoştinţă de articolele secrete, documentaţia tehnică şi alt tip de documentaţie trebuie să fie cît mai limitat şi se determină de către şeful subdiviziunii respective de producţie, de comun acord cu Subdiviziunea de protecţie.

623. Verificarea disponibilului articolelor avînd gradele de secretizare „Secret”, „Confidenţial” şi „Restricţionat” se efectuează cel puţin o dată în

trimestru, iar a celor cu parafa „Strict secret” – cel puţin o dată în lună.

624. Controlul general al disponibilului articolelor secrete se efectuează anual, în conformitate cu prevederile prezentului Regulament, de către comisii speciale, desemnate de către conducătorii autorităţilor publice şi ai altor persoane juridice respective.

Secţiunea a 2-a

Evidenţa articolelor secrete şi radierea lor din evidenţă

625. Articolele secrete se ţin în evidenţă atît în perioada elaborării, fabricării, păstrării, testării şi transportării, cît şi în perioada exploatării lor.

626. Autorităţile publice şi alte persoane juridice trebuie să întreprindă măsurile necesare ce ar exclude dezvăluirea informaţiei cu privire la existenţa articolelor secrete.

627. Evidenţa articolelor secrete se efectuează:

1) la producţia experimentală (în caz de lipsă a documentaţiei tehnologice) – de la începutul fabricării acesteia, conform schiţelor secrete, sau începînd cu etapa de producţie, indicată de constuctorul-elaborator sau de beneficiar;

2) la producţia în serie – din momentul indicat în fişele tehnologice sau de însoţire, iar în lipsa acestora – începînd cu etapa indicată în schiţă.

628. Articolele secrete recepţionate de la alte autorităţi sau persoane juridice se iau în evidenţă din momentul recepţionării lor.

629. Evidenţa articolelor secrete se ţine separat de evidenţa celor nesecrete, conform semnelor distinctive de pe schiţe, numerelor de uzină sau de inventar, care se aplică nemijlocit pe articole sau pe etichete speciale.

630. Articolele secrete pe care este imposibil de aplicat numere de evidenţă se iau în evidenţă cantitativ (spre exemplu: conform numărului de unităţi, conform greutăţii). Cele care se păstrează în ambalaj sigilat se iau în evidenţă conform numerelor de inventar aplicate pe marcajul ambalajului.

631. Numerotarea articolelor secrete se efectuează de către producător în modul care ar exclude posibilitatea de determinare a cantităţii totale a articolelor fabricate.

632. Modul de marcare a articolelor secrete se determină de comun acord cu beneficiarul.

633. Evidenţa articolelor secrete se efectuează conform registrelor luate în evidenţă de către Subdiviziunile de protecţie. Termenul de păstrare a acestor registre este de cel puţin 5 ani. În documentele de evidenţă pot fi indicate numai denumirile sau semnele convenţionale ale articolelor secrete.

634. Evidenţa, păstrarea şi controlul asupra circulaţiei articolelor secrete în

subdiviziunile autorităţii publice sau ale altei persoanei juridice se efectuează de către reprezentanţii Subdiviziunii de protecţie.

635. Şefii subdiviziunilor şi reprezentanţii Subdiviziunii de protecţie poartă răspundere personală pentru organizarea şi efectuarea evidenţei corespunzătoare a articolelor şi documentaţiei tehnice secrete în subdiviziuni şi la locurile de muncă.

636. Dacă la proiectarea şi fabricarea articolelor secrete sînt antrenate mai multe subdiviziuni, atunci se efectuează evidenţa centralizată a acestor articole, asigurînd controlul asupra circulaţiei fiecărui articol secret în subdiviziuni, din momentul înregistrării şi pînă la radierea din evidenţă.

637. Evidenţa centralizată se efectuează de către subdiviziunile de protecţie. Reprezentanţii Subdiviziunii de protecţie din cadrul subdiviziunilor de producţie informează regulat Subdiviziunea de protecţie despre circulaţia articolelor, pentru efectuarea înscrierilor corespunzătoare în Registrul de evidenţă a articolelor secrete (forma nr. 58, anexă la prezentul Regulament) sau în Registrul (Fişa) de evidenţă numerică a articolelor secrete (forma nr. 59, anexă la prezentul Regulament).

638. Articolele se eliberează executanţilor la locul de muncă în bază de semnătură (recipisă) în Registrul de evidenţă a articolelor secrete sau în Fişa de evidenţă pe articol (forma nr. 60, anexă la prezentul Regulament).

639. În cazul în care în baza particularităţilor procesului tehnologic de producţie (producere în masă) eliberarea contra semnătură a articolelor secrete executanţilor este imposibilă din cauza timpului redus de executare a operaţiunilor de către aceştia, în subdiviziuni (unităţi, sectoare) se numesc reprezentanţi ai subdiviziunilor de protecţie. Reprezentanţii subdiviziunilor de protecţie primesc articolele contra semnătură (recipisă) în Contul personal (forma nr. 29, anexă la prezentul Regulament) sau în Registrul de evidenţă privind eliberarea articolelor (forma nr. 61, anexă la prezentul Regulament) la locul de muncă, efectuînd controlul asupra disponibilului şi circulaţiei acestora.

640. Transmiterea articolelor de la un sector de producţie la altul se efectuează potrivit registrului din forma nr. 62, anexă la prezentul Regulament, care este ţinut în subdiviziunea respectivă de reprezentanţii Subdiviziunii de protecţie şi serveşte drept bază pentru anularea semnăturii de primire a articolelor în Registrul de evidenţă privind eliberarea articolelor sau în Contul personal şi plasarea fişelor de evidenţă pe articol dintr-un sector al fişierului în altul.

641. Predarea articolelor secrete pe schimburi se efectuează de persoanele responsabile pentru evidenţa şi păstrarea lor, contra semnătură (recipisă). Disponibilul articolelor predate se verifică conform unităţilor, după numere sau greutate.

642. Predarea articolelor secrete dintr-o subdiviziune în alta se efectuează prin intermediul reprezentantului Subdiviziunii de protecţie, în baza sarcinii

(planului) de producţie, conform Foii de însoţire (forma nr. 63, anexă la prezentul Regulament), cu informarea Subdiviziunii de protecţie despre acest fapt.

643. Schiţele şi documentaţia tehnică, de cercetare ştiinţifică, precum şi altă documentaţie prevăzută pentru crearea articolelor secrete se eliberează la locurile de muncă contra semnătură (recipisă) şi numai pentru orele de muncă ale schimbului.

644. Se interzice predarea articolelor şi documentaţiei tehnice secrete sau altei documentaţii secrete ce se referă la aceste articole dintr-o subdiviziune în alta, eludînd Subdiviziunea de protecţie sau reprezentanţii acesteia.

645. Pentru montarea blocurilor, reţelelor şi detaliilor secrete în articole se întocmeşte un proces-verbal, conform formei nr.64, anexă la prezentul Regulament, într-un singur exemplar, care se aprobă de şeful subdiviziunii, iar la experimentări – de către conducătorul tehnic sau de constructorul principal. Numerele de evidenţă ale blocurilor, reţelelor şi detaliilor se înscriu în paşaportul tehnic (formularul) al articolului. Procesele-verbale şi înscrierile efectuate în paşapoartele tehnice (formulare) se confirmă prin semnătura persoanelor responsabile de montare. În cazul retragerii sau înlocuirii elementelor secrete de completare se întocmeşte un proces-verbal, conform formei nr. 65, anexă la prezentul Regulament, care serveşte temei pentru luarea în evidenţă a articolului sau pentru includerea lui în procesul-verbal cu privire la distrugere.

646. În cazul în care, conform condiţiilor de fabricare, în tipul schimbului de muncă se efectuează de mai multe ori montarea şi retragerea elementelor secrete de completare cu scopul de a obţine caracteristicile necesare ale articolului în care ele se montează, procesul-verbal cu privire la montare se întocmeşte numai pentru elementul montat definitiv, iar apoi se fac înscrierile respective în documentele luate în evidenţă.

647. Persoanele care au efectuat montarea elementelor de completare, imediat după întocmirea procesului-verbal respectiv, sînt obligate să predea elementele nepotrivite reprezentantului Subdiviziunii de protecţie.

648. Pentru toate articolele secrete sau lotul de articole secrete fabricate se întocmesc paşapoarte tehnice. Dacă datele înscrise în paşaportul tehnic conţin informaţii secrete, atunci acestuia i se atribuie parafa de secretizare respectivă şi numărul din Registrul evidenţei de inventar a documentaţiei tehnice secrete, care se înscrie în registrele respective, în care a fost luat în evidenţă articolul (Registrul de evidenţă a articolelor secrete sau Registrul (Fişa) de evidenţă numerică a articolelor secrete).

649. Efectuarea ştersăturilor în orice formă în documentaţia cu privire la evidenţa articolelor secrete nu se admite. În caz de necesitate, operarea unor modificări în această documentaţie se legalizează prin semnătura persoanei care le-a efectuat, cu indicarea datei.

650. Articolele secrete se radiază din evidenţă la transmiterea lor în alte autorităţi publice sau persoane juridice, distrugerea acestora, consumarea lor în procesul testărilor şi altor lucrări, montării lor în alte articole sau la desecretizarea acestora.

651. Temei pentru radierea articolului secret din evidenţă serveşte:

1) recipisa destinatarului în foaia de însoţire, legalizată prin ştampilă sau confirmată prin procura de primire a documentelor secrete;

2) procesul-verbal cu privire la distrugerea articolelor secrete;

3) procesul-verbal cu privire la consumarea articolelor secrete în timpul efectuării lucrărilor de testare şi a altor lucrări;

4) procesul-verbal cu privire la montarea articolelor de completare;

5) decizia cu privire la desecretizare.

Secţiunea a 3-a

Păstrarea articolelor secrete

652. Articolele secrete se păstrează în încăperi (depozite, arhive, încăperi accesorii) care corespund cerinţelor prezentului Regulament.

653. Articolele secrete se păstrează separat de cele nesecrete. În cazurile în care articolele nesecrete constituie o parte a articolului secret, ele pot fi păstrate împreună cu articolele secrete.

654. În încăperile unde se păstrează articolele secrete, accesul persoanelor care nu lucrează aici, dar care dispun de dreptul de acces la secret de stat de forma corespunzătoare, se înfăptuieşte în modul următor:

1) în depozitele din secţie şi depozitele uzinei – conform listei aprobate de şeful secţiei sau depozitului respectiv, coordonate cu şeful Subdiviziunii de protecţie;

2) în depozitele de producţie finită avînd gradul de secretizare „Strict secret” – cu permisiunea scrisă a conducătorului persoanei juridice.

655. În procesul activităţii sau a testării se permite păstrarea articolelor secrete la locurile de muncă, sub responsabilitatea executanţilor şi a şefilor subdiviziunilor respective de producţie.

656. În afara orelor de muncă, articolele secrete trebuie păstrate în depozite speciale, care se încuie şi se sigilează de către persoanele responsabile pentru păstrarea lor.

657. Depozitele destinate pentru păstrarea producţiei cu gradul de secretizare „Strict secret” trebuie să fie amplasate în locuri separate, izolate de sarcinile de producţie, înzestrate cu mijloace tehnice de pază, comunicaţie şi antiincendiare.

658. În afara programului de lucru, la locurile de muncă sau pe standurile de testare pot să rămînă articolele a căror testare tehnologică sau operaţiune nu poate fi întreruptă, precum şi articolele de gabarit mare. Ele trebuie să se păstreze în adăposturi montabile-demontabile de metal, lemn, cauciuc, prelată sau în alte adăposturi sigilate, care ar asigura integritatea şi camuflarea acestora.

659. Lista articolelor secrete cu indicarea locurilor de păstrare a acestora se aprobă de către şeful autorităţii publice sau al altei persoane juridice, după coordonarea cu şeful Subdiviziunii de protecţie.

Secţiunea a 4-a

Primirea şi transmiterea articolelor secrete

660. Reprezentanţii autorităţilor publice sau ai altor persoane juridice, destinatari ai articolelor secrete, trebuie să aibă procură, perfectată în modul stabilit, legalizată prin ştampila autorităţii sau a altei persoane juridice respective. Procurile sînt vizate de către şeful Subdiviziunii de protecţie.

661. Primirea (predarea) articolelor secrete se efectuează în baza Foii de însoţire (forma nr.66, anexă la prezentul Regulament), actului de predare-primire şi altor documente de însoţire, verificîndu-se în mod obligatoriu integritatea ambalajului şi a plumburilor. Numărul de plumburi, a cleştelor de plumbuit şi descrierea amprentelor acestora se indică în documentele de însoţire.

662. La depistarea semnelor de deschidere a vagoanelor, a ambalajului sau în cazul unor defecte ale amprentelor sigiliilor (plumburilor), persoanele care efectuează primirea (predarea) articolelor secrete întocmesc un proces-verbal. Faptele enunţate se comunică imediat expeditorului, autorităţii cu împuterniciri de dispoziţie asupra acestor informaţii şi Serviciului de Informaţii şi Securitate.

663. Deschiderea coletelor şi a ambalajului, confruntarea articolelor secrete primite cu informaţia indicată în documentele de însoţire, verificarea stării şi integrităţii acestora se efectuează de către persoanele responsabile de evidenţa şi păstrarea articolelor secrete şi de către reprezentanţii subdiviziunii controlului tehnic.

664. Dacă în procesul verificării se depistează lipsa unor articole sau încălcarea integrităţii acestora, atunci se întocmeşte un proces-verbal, un exemplar fiind remis expeditorului pentru întreprinderea măsurilor de rigoare.

665. Autorităţile publice sau alte persoane juridice care au primit din greşeală articole secrete ce nu le aparţin sînt obligate să le primească spre păstrare provizorie, dacă stabilirea adresei destinatarului şi expedierea imediată a acestora potrivit destinaţiei nu este posibilă. Deschiderea ambalajului unor astfel de articole este interzisă.

666. În cazul în care în baza documentelor de însoţire nu se poate determina caracterul articolelor secrete primite din greşeală sau pericolul de explozie al acestora, atunci păstrarea

lor pînă la momentul transmiterii se va face separat de alte articole.

667. Transmiterea articolelor secrete se efectuează cu permisiunea scrisă a conducătorului autorităţii publice sau al altei persoane juridice, conform foii de însoţire.

668. Pentru comanda mijloacelor de transport şi a corpului de pază, necesare pentru însoţirea articolelor în timpul transportării, se eliberează dispoziţia de expediere pentru livrarea articolelor secrete, conform formei nr. 67, anexă la prezentul Regulament.

669. Drept temei pentru scoaterea articolelor secrete de pe teritoriul păzit al autorităţii publice sau al altei persoane juridice serveşte permisul special semnat de către şeful de producţie, şeful secţiei şi şeful Subdiviziunii de protecţie, în baza foii de însoţire şi dispoziţiei de expediere pentru livrarea articolelor secrete.

670. Documentaţia de exploatare şi reparaţie necesară pentru articolele secrete transmise se expediază prin poşta specială, concomitent cu articolele. În anumite cazuri se admite expedierea acestei documentaţii prin intermediul persoanei care însoţeşte articolele secrete şi are procură întocmită în modul stabilit de prezentul Regulament.

671. La transmiterea articolelor secrete, în documentele de însoţire (spre exemplu, scrisori de însoţire, foi de ambalaj (forma nr. 68, anexă la prezentul Regulament), paşapoarte tehnice) trebuie să fie înscrise acele denumiri sau semne convenţionale ale articolelor care sînt indicate în marcările lor.

672. În documentele de transport şi financiar-contabile se indică denumirile sau semnele convenţionale ale articolelor şi numărul acestora. Pentru confirmarea transmiterii încărcăturii, pe aceste documente se indică numerele de ieşire ale documentelor de însoţire.

Secţiunea a 5-a

Transportarea articolelor secrete

673. Transportarea articolelor secrete, coletelor poştale cu valoare declarată, încasărilor şi corespondenţei speciale se efectuează de către persoanele responsabile care au drept de acces la secretul de stat de forma respectivă, numite de conducătorii autorităţilor publice sau ai altor persoane juridice.

674. Persoanele responsabile de transportarea articolelor secrete, coletelor poştale cu valoare declarată, încasărilor şi corespondenţei speciale trebuie să cunoască şi să respecte cu stricteţe regulile de pază şi tehnica securităţii, să păstreze caracterul secret în procesul transportării.

675. Locurile destinate pentru lucrările de încărcare-descărcare a articolelor secrete trebuie să fie protejate sigur, pentru a exclude posibilitatea examinării vizuale sau prin mijloace tehnice de către persoane străine.

676. Articolele secrete supuse transportării trebuie să fie împachetate în aşa fel încît să se excludă posibilitatea determinării caracterului acestora. În acelaşi mod vor fi împachetate şi articolele nesecrete transportate, dispozitivele, utilajul, care după aspectul lor exterior pot determina caracterul articolelor secrete pentru care sînt destinate.

677. Vagoanele destinate transportării articolelor secrete nu trebuie să se deosebească, după aspectul lor exterior, de vagoanele destinate transportării articolelor nesecrete.

678. Pe vagoanele în care sînt transportate articolele secrete nu se scrie denumirea staţiilor de plecare şi de destinaţie, denumirea încărcăturilor şi a destinatarilor.

679. Paza înarmată a articolelor secrete la transportare se va asigura în funcţie de gradul de secretizare a acestora.

680. Călătoria unor persoane străine împreună cu încărcătura păzită este interzisă.

681. Distribuirea articolelor secrete, coletelor poştale cu valoare declarată, încasărilor şi corespondenţei speciale prin intermediul Serviciului de Stat de Curieri Speciali se efectuează în modul stabilit de prezentul Regulament.

Secţiunea a 6-a

Testarea articolelor secrete

682. Testarea articolelor secrete se efectuează în locuri special repartizate în aceste scopuri, care se asigură cu pază.

683. Pînă la începerea lucrărilor de testare se iau măsuri în vederea excluderii posibilităţii de examinare vizuală sau prin mijloace tehnice, de către persoane străine, a articolelor secrete supuse testărilor şi a rezultatelor acestora.

684. Acţiunile concrete cu privire la asigurarea regimului secret pe parcursul testărilor, precum şi cerinţele privind eficacitatea acestora se includ în programele de testări.

685. La lucrările de testare a articolelor secrete pot asista numai persoanele cu drept de acces la secretul de stat, care au atribuţie directă la acestea.

686. Participanţii la testări pot lua cunoştinţă numai de acele informaţii cu privire la caracterul şi rezultatul testărilor care se referă nemijlocit la activitatea îndeplinită de către ei în cadrul testării respective.

687. Documentaţia de construcţie şi exploatare a articolelor secrete trebuie să conţină metode de verificare şi indicaţii cu privire la pregătirea aparatelor de măsurat, care în timpul măsurării (testării) parametrilor articolelor secrete nu ar dezvălui conţinutul informaţiilor secrete, neprevăzute de verificare.

688. Punerea în funcţiune de probă, testarea şi exploatarea articolelor secrete trebuie să se efectueze în condiţii care ar exclude pierderea eventuală a informaţiei secrete prin canale tehnice.

689. Pentru articolele secrete consumate în procesul testărilor sau al altor lucrări experimentale se întocmeşte un proces-verbal, care serveşte temei pentru trecerea acestora la pierderi şi radierea din evidenţă.

690. Dacă în baza resturilor inutilizabile de la articolele secrete pot fi determinate caracteristicile secrete sau destinaţia specială a articolelor respective, aceste resturi se supun distrugerii. În acest scop, la finisarea testării se va examina locul de testare a articolelor secrete pentru identificarea şi distrugerea resturilor respective, iar cu privire la rezultatele acestei examinări se va întocmi un proces-verbal.

691. În timpul testărilor, comisiile de stat (de recepţie) apreciază eficacitatea acţiunilor cu privire la asigurarea caracterului secret al acestora, reflectînd rezultatele acestei aprecieri în documentele de dare de seamă.

Secţiunea a 7-a

Distrugerea articolelor secrete

692. Sînt supuse distrugerii articolele secrete rebutate în procesul de producţie, de testare şi de exploatare sau articolele secrete care şi-au pierdut necesitatea practică.

693. Selectarea şi distrugerea articolelor secrete se efectuează de către o comisie special instituită în acest scop, cu participarea unui angajat sau reprezentant al Subdiviziunii de protecţie, în baza unui proces-verbal cu privire la distrugerea articolelor secrete (forma nr. 69, anexă la prezentul Regulament).

694. Procesul-verbal de distrugere a articolelor secrete se aprobă de către conducătorul autorităţii publice sau al altei persoane juridice, iar în unele cazuri, cu permisiunea acestuia – de către şefii subdiviziunilor de producţie.

695. După aprobarea procesului-verbal, distrugerea articolelor secrete (demontarea, desfacerea, distrugerea sau deformarea) se efectuează conform tehnologiei menţionate de elaborator în paşaportul tehnic al articolului secret. Modalitatea de distrugere a articolelor secrete trebuie să facă imposibilă restabilirea caracteristicilor autentice, parametrilor sau destinaţiei lor speciale.

696. Faptul distrugerii se consemnează în procesul-verbal, prin semnăturile persoanelor care au efectuat distrugerea.

697. Paşapoartele tehnice ale articolelor secrete distruse la fel sînt supuse distrugerii, în modul stabilit de prezentul Regulament, cu consemnarea acestui fapt în procesul-verbal cu privire la distrugerea articolelor secrete.

698. În procesul-verbal cu privire la distrugerea articolelor secrete se reflectă, de asemenea, faptul retragerii pieselor de completare secrete utilizabile din

articolele distruse, care se iau în evidenţa corespunzătoare.

699. Blocurile, detaliile şi materialele nesecrete utilizabile pot fi retrase din articolele secrete supuse distrugerii şi transmise, conform foilor de însoţire, la depozitele generale pentru utilizarea lor ulterioară în procesul de producţie.

700. Din articolele secrete supuse distrugerii se retrag, în mod obligatoriu, metalele preţioase.

701. Procesele-verbale cu privire la distrugerea articolelor secrete se păstrează în dosare speciale cel puţin 5 ani. Gradul de secretizare a acestora se determină în funcţie de informaţiile pe care le conţin.

Capitolul VII

REGULI DE OPERARE CU CORESPONDENŢA CIFRATĂ ÎN AUTORITĂŢILE PUBLICE SAU ALTE PERSOANE JURIDICE

Secţiunea 1

Dispoziţii generale

702. Utilizarea mijloacelor de comunicaţii cifrate se admite numai în cazul în care nu există posibilitate sau nu este raţional a transmite informaţia urgentă referitor la problemele secrete, precum şi informaţia urgentă nesecretă interzisă de a fi transmisă în formă deschisă prin mijloace tehnice neprotejate, prin intermediul altor mijloace de comunicaţie.

703. Organizarea şi efectuarea întregului complex de lucrări ce ţin de corespondenţa cifrată se pune în sarcina organelor de cifrare ale autorităţilor publice sau ale altor persoane juridice – subdiviziuni, amenajate cu aparatajul respectiv (mijloace de comunicaţii cifrate).

704. Organizarea, funcţiile, drepturile, obligaţiile organelor de cifrare se stabilesc în regulamentul de funcţionare al acestora, elaborat în conformitate cu cerinţele prezentului Regulament, coordonat cu Serviciul de Informaţii şi Securitate şi aprobat de conducătorul autorităţii publice sau al altei persoane juridice.

705. Crearea, reorganizarea şi lichidarea organelor de cifrare se efectuează în baza deciziei (ordinului) conducătorilor autorităţilor publice sau a altor persoane juridice, prin coordonare cu Serviciul de Informaţii şi Securitate. La crearea noilor organe de cifrare, Serviciul de Informaţii şi Securitate verifică existenţa condiţiilor necesare pentru asigurarea regimului secret la organizarea lucrărilor cu corespondenţa cifrată a acestora.

706. În funcţie de specificul activităţii şi volumul informaţiilor vehiculate,

în cadrul autorităţilor publice sau al altor persoane juridice lucrările ce ţin de corespondenţa cifrată pot fi realizate de către o persoană numită special de către conducătorii acestora. În acest caz, atribuţiile organului de cifrare vor fi îndeplinite de această persoană, care va efectua primirea şi transmiterea corespondenţei cifrate nemijlocit, prin utilizarea aparatajului respectiv.

707. În autorităţile publice sau alte persoane juridice în care lipsesc organele de cifrare lucrările ce se referă la corespondenţa cifrată (întocmire, evidenţă, utilizare, transmitere, păstrare şi distrugerea mesajelor cifrate) se pun în sarcina Subdiviziunii de protecţie a acestora. Ultima efectuează primirea şi transmiterea corespondenţei cifrate, prin intermediul organelor de cifrare ale altor autorităţi publice sau persoane juridice.

Secţiunea a 2-a

Reguli generale de operare cu corespondenţa cifrată în autorităţile publice sau alte persoane juridice în care lipsesc organele de cifrare

708. Modul de întocmire, evidenţă, utilizare, transmitere, păstrare şi distrugere a mesajelor cifrate trebuie să asigure integritatea acestora şi să excludă posibilitatea divulgării informaţiilor ce le conţin.

709. Evidenţa şi păstrarea mesajelor cifrate, precum şi aducerea conţinutului acestora la cunoştinţa persoanelor cărora le sînt adresate şi executanţilor se efectuează de către şeful Subdiviziunii de protecţie sau de o persoană desemnată din cadrul acesteia.

710. Mesajele cifrate, registrele de evidenţă şi alte documente ce se referă la corespondenţa cifrată se păstrează de către Subdiviziunea de protecţie în safeuri sau dulapuri de metal.

711. Acces la mesajele cifrate avînd gradele de secretizare „Strict secret”, „Secret”, „Confidenţial”, „Restricţionat” au doar persoanele care, potrivit caracterului obligaţiilor de serviciu, au atribuţie nemijlocită la acestea şi dispun de dreptul de acces la secretul de stat de forma respectivă. Numărul acestor persoane trebuie să fie limitat.

712. Subdiviziunea de protecţie deţine lista persoanelor care au acces la lucrul cu corespondenţa cifrată, aprobată de conducătorul autorităţii publice sau al altei persoane juridice, în care se menţionează, inclusiv, persoanele cu drept de a semna mesajele cifrate de ieşire. La necesitate, lista se actualizează în cel mai scurt termen posibil.

713. La prelucrarea mesajelor cifrate, persoanele sînt admise numai după un instructaj detaliat şi după familiarizarea, contra semnătură, cu procedura de utilizare a mesajelor cifrate.

714. Persoanele care lucrează cu mesajele cifrate nu au dreptul să divulge

informaţiile cunoscute din corespondenţa cifrată, să poarte discuţii cu privire la conţinutul mesajelor cifrate, în cazul utilizării canalelor de comunicaţii neprotejate, să păstreze la sine ciornele mesajelor cifrate, să facă înscrieri neautorizate despre conţinutul mesajelor cifrate în caiete de lucru, carnete, pe file neînregistrate, să transmită unul şi acelaşi text al mesajului în mod deschis şi cifrat.

715. Executanţii şi reprezentanţii altor autorităţi publice sau persoane juridice pot lua cunoştinţă de conţinutul mesajelor cifrate numai conform indicaţiei în scris a destinatarului sau a persoanelor care au semnat mesajul cifrat. Reprezentanţii altor autorităţi publice sau persoane juridice trebuie să prezinte certificatul de acces de forma respectivă şi actele de identificare.

716. Conţinutul mesajelor cifrate poate fi făcut public în cadrul şedinţelor, adunărilor, a altor întruniri, numai dacă toţi participanţii la acestea au dreptul de acces la secretul de stat de forma respectivă.

717. Se interzice a face referire la faptul că informaţiile sînt primite prin corespondenţă cifrată.

718. Controlul asupra respectării regulilor cu privire la întocmirea, evidenţa, păstrarea, utilizarea corespondenţei cifrate în cadrul autorităţilor publice şi altor persoane juridice se asigură de către subdiviziunile de protecţie şi conducătorii acestora.

719. Verificarea disponibilului mesajelor cifrate în autorităţile publice şi alte persoane juridice se efectuează în modul stabilit pentru documentele secrete.

Secţiunea a 3-a

Reguli de transmitere a mesajelor cifrate în autorităţile publice sau alte persoane juridice care nu dispun de organe de cifrare

720. Întocmirea mesajelor cifrate de ieşire (forma nr. 70, anexă la prezentul Regulament) se efectuează în condiţii care exclud posibilitatea divulgării conţinutului acestora unor persoane care nu au atribuţie la ele.

721. Dreptul de a semna mesajele cifrate de ieşire se acordă conducătorilor autorităţilor publice sau ai altor persoane juridice, adjuncţilor acestora sau, cu permisiunea conducătorilor, altor persoane cu funcţii de conducere (şefi de subdiviziuni).

722. Semnătura persoanei cu funcţie de răspundere de pe mesajul cifrat de ieşire, remisă pentru transmitere organului de cifrare al altei autorităţi publice sau persoane juridice, se legalizează prin ştampila autorităţii publice sau persoanei juridice respective.

723. Mesajele cifrate de ieşire se scriu de mînă sau cu utilizarea mijloacelor tehnice pe blanchete, ţinute în evidenţă prealabilă, într-un singur exemplar, lizibil, succint, fără utilizarea prescurtărilor libere ale cuvintelor. Se admite

întocmirea mesajelor cifrate pe file luate în evidenţă de către Subdiviziunea de protecţie, pe care se va aplica menţiunea „Mesaj cifrat". Sub formularul sau fila pe care se întocmeşte mesajul cifrat trebuie să fie plasat un suport rigid (garnitură), care ar exclude imprimarea textului mesajului pe alte formulare sau file. La întocmirea mesajelor cifrate cu utilizarea mijloacelor tehnice, suportul rigid (garnitura) nu se foloseşte.

724. Se interzice întocmirea mesajelor cifrate în cîteva exemplare, precum şi multiplicarea acestora.

725. Toate rectificările şi completările operate în text se stipulează şi se legalizează prin semnătura executantului sau a persoanei care semnează mesajul cifrat.

726. Mesajele cifrate de ieşire, întocmite ilizibil, inclusiv cele care conţin rectificări nestipulate, nu sînt admise pentru expediere.

727. Blanchetele destinate pentru întocmirea mesajelor cifrate se broşează în carnete, care se trec în evidenţă în Registrul de evidenţă a caietelor de lucru. Filele acestor carnete se numerotează. Eliberarea carnetelor sau a unor blanchete aparte executanţilor, precum şi restituirea acestora Subdiviziunii de protecţie se efectuează contra semnătură (recipisă) în registrul de evidenţă.

728. Pe mesajele cifrate de ieşire se aplică parafa de secretizare, menţiunea cu privire la caracterul urgent (prioritar) al mesajului cifrat, numele, prenumele, funcţia destinatarului, numele, prenumele, funcţia persoanei care a semnat mesajul cifrat, data semnării, numărul de înregistrare, numele, prenumele executantului.

729. Gradul de secretizare şi caracterul urgent se determină de către executant sau persoana care a semnat mesajul cifrat.

730. Mesajele cifrate de ieşire, transmise la doi şi mai mulţi destinatari, se întocmesc într-un singur exemplar, cu indicarea tuturor destinatarilor. În caz de necesitate (cînd există mai mulţi destinatari), pe verso mesajului cifrat sau pe o foaie separată se întocmeşte lista de expediere, care se legalizează prin semnătura executantului sau a persoanei care semnează mesajul cifrat.

731. Mesajele cifrate, care conţin informaţii secretizate cu parafa „Strict secret", se transmit prin intermediul organelor de cifrare ale altor autorităţi publice sau persoane juridice numai în cazuri excepţionale, la indicaţia scrisă a conducătorului autorităţii publice sau persoanei juridice care le-a semnat.

732. Întocmirea mesajelor cifrate de ieşire avînd gradul de secretizare „Strict secret" poate fi efectuată doar cu permisiunea conducătorului autorităţii publice sau al altei persoane juridice. Acestea se înregistrează în Subdiviziunea de protecţie , fiind comunicate de executant.

733. Pentru a fi transmise către anumiţi destinatari, mesajele cifrate avînd

gradul de secretizare „Strict secret” se prezintă Subdiviziunii de protecţie în plicuri sigilate, care conţin, după caz, pe lîngă parafa de secretizare, şi menţiunea „Personal” sau „Strict personal”.

734. Mesajele cifrate de ieşire se predau de către executant Subdiviziunii de protecţie. Blanchetele şi filele luate în evidenţă, deteriorate în procesul întocmirii mesajelor cifrate, se restituie Subdiviziunii de protecţie pentru a fi distruse în modul stabilit de prezentul Regulament.

735. Mesajele cifrate de ieşire se înregistrează în Registrul de evidenţă a mesajelor transmise (forma nr. 71, anexă la prezentul Regulament).

736. După înregistrare, mesajele se transmit imediat organului de cifrare respectiv, într-un plic sigilat.

737. Pe plic se indică adresa destinatarului şi a expeditorului, numărul mesajului cifrat, parafa de secretizare, menţiunea cu privire la caracterul urgent (prioritar) al mesajului şi menţiunea „Mesaj cifrat”. După cifrare, mesajele destinate transmiterii rămîn la organul de cifrare.

738. Transmiterea şi distribuirea plicurilor cu mesajele cifrate se efectuează în modul stabilit pentru transmiterea şi distribuirea documentelor secrete.

Secţiunea a 4-a

Reguli de recepţionare a mesajelor cifrate în autorităţile publice sau alte persoane juridice care nu dispun de organe de cifrare

739. Plicurile cu mesajele cifrate primite de autorităţile publice sau alte persoane juridice se înregistrează imediat în Registrul de control al plicurilor şi se transmit persoanei responsabile pentru evidenţa şi păstrarea corespondenţei cifrate, contra semnătură (recipisă) în acest registru, indicîndu-se data şi ora primirii plicului.

740. După deschiderea plicurilor, mesajele cifrate se înregistrează în Registrul de evidenţă a mesajelor cifrate primite (forma nr. 72, anexă la prezentul Regulament). Dacă în plic există cîteva mesaje cifrate, fiecare dintre ele se înregistrează cu un număr de intrare aparte. Se interzice de a comunica şi de a transmite executanţilor mesajele cifrate care nu au fost luate în evidenţă.

741. Rezoluţiile se aplică nemijlocit pe mesajele cifrate. Aplicarea rezoluţiilor pe file separate nu se admite.

742. Transmiterea mesajelor cifrate în interiorul autorităţii publice sau al altei persoane juridice se efectuează numai prin intermediul Subdiviziunii de protecţie, iar în afara acestora – prin intermediul organului de cifrare.

743. Mesajele cifrate pot avea menţiunile „Personal” sau „Strict personal”. Plicurile cu mesajele cifrate cu menţiunea „Personal” se deschid de către

destinatar sau de către persoana împuternicită de acesta, iar plicurile cu menţiunea „Strict personal” se deschid numai de către destinatar şi doar ca excepţie (în cazul în care lipseşte destinatarul) pot fi deschise de către persoana care-l înlocuieşte. În registrul de evidenţă a mesajelor cifrate primite se înscrie: „Plic cu menţiunea „Personal” sau „Plic cu menţiunea „Strict personal”. Alte menţiuni cu privire la mesajele cifrate se efectuează în registru din spusele destinatarului sau executantului. Ştampila de înregistrare se aplică pe plic, indicîndu-se numărul de intrare şi data. Persoana care deschide plicul trece aceste date pe mesajul cifrat.

744. Informarea cu conţinutul mesajelor cifrate care au gradul de secretizare „Strict secret” se permite doar cu permisiunea scrisă a conducătorului autorităţii publice sau al altei persoane juridice, numai a persoanelor care au nevoie să cunoască conţinutul acestora, reieşind din atribuţiile exercitate şi care au drept de acces la secretul de stat de forma respectivă.

745. Eliberarea mesajelor cifrate executanţilor pentru lucru şi recepţionarea acestora se efectuează contra semnătură (recipisă) în Registrul de evidenţă a mesajelor cifrate primite. Se interzice de a transmite mesajele cifrate de la unii executanţi către alţii, cu eludarea Subdiviziunii de protecţie.

746. Persoanele care au luat cunoştinţă de conţinutul mesajelor cifrate semnează lizibil pe acestea, indicînd data, după caz, ora cînd au luat cunoştinţă.

747. Pe mesajele cifrate, executanţii sînt obligaţi să facă însemnări cu privire la executarea acestora, pe care le confirmă prin semnătură, indicînd data, după caz, ora executării.

748. După dispariţia necesităţii de a lucra cu mesajele cifrate, acestea se restituie imediat Subdiviziunii de protecţie.

749. Mesajele cifrate se clasează în dosare numai cu însemnările respective privind executarea lor.

750. Din conţinutul mesajelor cifrate, cu excepţia celor avînd gradul de secretizare „Strict secret”, pot fi efectuate însemnări succinte în carnete speciale cu file detaşabile. Aceste carnete se iau în evidenţă de către Subdiviziunea de protecţie şi se eliberează executanţilor contra semnătură. Filele carnetelor speciale ce conţin înscrieri inutilizabile în activitatea ulterioară se extrag periodic şi se distrug.

751. În caz de necesitate, reieşind din conţinutul mesajelor cifrate de ieşire şi de intrare, cu excepţia celor care au gradul de secretizare „Strict secret”, pot fi întocmite informaţii sumare sau extrase care se iau în evidenţă de către Subdiviziunea de protecţie, se păstrează şi se distrug în modul stabilit pentru documentele cu gradul de secretizare respectiv.

752. Despre întocmirea informaţiilor sau extraselor pe mesajele cifrate respective şi în registrele de evidenţă a acestora se efectuează însemnări cu

privire la numărul de exemplare întocmite şi numărul de evidenţă al acestora.

753. Cu permisiunea conducătorilor autorităţilor publice sau a altor persoane juridice, informaţiile ce le conţin mesajele cifrate, cu excepţia celor avînd parafa de secretizare „Strict secret", pot fi incluse în alte documente secrete, cu condiţia ca gradul de secretizare a acestora să nu fie mai înalt decît gradul de secretizare a documentelor în care se includ informaţiile. Despre includerea acestor informaţii în documentele secrete, pe mesajele cifrate respective şi în registrele de evidenţă ale acestora, se fac însemnări, indicîndu-se numerele de evidenţă ale documentelor în care au fost incluse.

754. Mesajele cifrate de intrare care au fost executate se restituie, în cel mai scurt termen, organelor de cifrare de la care au fost primite. În unele cazuri, atunci cînd există acordul comun al autorităţilor publice sau al altor persoane juridice şi permisiunea organelor respective ale securităţii statului, mesajele cifrate, cu excepţia celor care au gradul de secretizare „Strict secret", pot fi păstrate de către subdiviziunile de protecţie, în dosare aparte. Termenele de păstrare a mesajelor cifrate în autorităţile publice sau alte persoane juridice se determină de către conducătorii acestora şi trebuie să fie minime. La dispariţia necesităţii de a lucra în continuare cu mesajele cifrate sau la expirarea termenului de păstrare al acestora, mesajele cifrate se distrug, cu permisiunea conducătorului autorităţii publice sau al altei persoane juridice, în modul stabilit pentru distrugerea documentelor secrete. Mesajele cifrate avînd gradul de secretizare „Strict secret" se restituie organului de cifrare.

Capitolul VIII

REGULI DE DESFĂŞURARE A REUNIUNILOR SECRETE

755. Reuniunile de serviciu în cadrul cărora se examinează chestiuni secrete se desfăşoară cu permisiunea conducătorilor autorităţilor publice sau ai altor persoane juridice, care desemnează persoana responsabilă de organizarea unor astfel de reuniuni.

756. Persoana responsabilă de organizarea reuniunilor secrete, în comun cu Subdiviziunea de protecţie şi specialiştii tehnici respectivi, întreprind măsurile organizatorice şi tehnice de securitate, care asigură păstrarea caracterului secret al chestiunilor puse în discuţie şi exclude posibilitatea de divulgare sau pierdere a informaţiilor atribuite la secret de stat în timpul desfăşurării acestora. Abordarea chestiunilor secrete curente în cadrul reuniunilor care nu implică reprezentanţi ai altor autorităţi sau persoane juridice poate fi efectuată sub conducerea şefilor de subdiviziuni ai autorităţii publice sau al altei persoane juridice respective, fără implicarea Subdiviziunii de protecţie.

757. Măsurile de securitate se axează în special pe:

1) măsuri de protecţie la locul reuniunii pentru a se asigura că aceasta se desfăşoară fără nici un incident care ar putea compromite securitatea

informaţiilor atribuite la secret de stat;

2) controlul personalului care are acces la locul reuniunii şi verificarea materialelor introduse în încăperea destinată reuniunii;

3) coordonarea cu autorităţile publice şi alte persoane juridice, care urmează să delege participanţi la reuniune;

4) stabilirea unor instrucţiuni de securitate (includerea acestora în materialele destinate reuniunii sau comunicarea conţinutului acestora participanţilor).

758. Responsabilitatea pentru asigurarea regimului secret în cadrul reuniunilor secrete o poartă autoritatea publică sau persoana juridică organizatoare.

759. La reuniuni se admit numai persoanele care au acces la secretul de stat de forma corespunzătoare gradului de secretizare a chestiunilor ce urmează a fi puse în discuţie. Reprezentanţii altor autorităţi publice sau persoane juridice prezintă, pînă la deschiderea reuniunii, subdiviziunii de protecţie a organizatorului certificatele de acces la secretul de stat de forma corespunzătoare.

760. La întocmirea programului (ordinii de zi) privind desfăşurarea reuniunii secrete se va ţine cont de succesiunea abordării subiectelor, pentru a exclude participarea la discuţie a persoanelor care nu au atribuţie sau acces la aceste probleme.

761. Persoana responsabilă de organizarea reuniunii trebuie să prezinte Subdiviziunii de protecţie programul de desfăşurare a reuniunii şi lista participanţilor cu indicarea numelui, prenumelui, funcţiei (instituţiei al cărei reprezentant este) formei de acces, subiectele la abordarea cărora urmează să participe.

762. Lista persoanelor invitate la reuniune este coordonată de către persoana responsabilă de organizarea reuniunii cu Subdiviziunea de protecţie şi se aprobă de către conducătorul autorităţii publice sau al altei persoane juridice care a permis desfăşurarea reuniunii.

763. Participanţii vor fi admişi la reuniune conform listei, la prezentarea actelor de identificare (documentelor de legitimare). Acestora li se pot elibera permise speciale de acces la reuniune.

764. Materialele secrete necesare pentru desfăşurarea reuniunii se expediază persoanelor invitate conform listei aprobate de către conducătorul autorităţii publice sau al altei persoane juridice care a permis organizarea acesteia. Participanţilor li se expediază doar acele materiale care ţin de chestiunile ce-i vizează nemijlocit. Asigurarea controlului privind restituirea în termen a acestor materiale este pusă în sarcina Subdiviziunii de protecţie.

765. Persoana responsabilă de organizarea reuniunii, la deschiderea acesteia, va anunţa gradul de secretizare a reuniunii în scopul excluderii posibilităţii de divulgare a informaţiilor şi preîntîmpinării participanţilor despre efectuarea

înscrierilor secrete numai în caietele de lucru luate în evidenţă şi eliberate de Subdiviziunea de protecţie înainte de începerea reuniunii. În timpul unor întreruperi îndelungate, precum şi la finele reuniunii, caietele de lucru se predau subdiviziunii de protecţie.

766. Decizia adoptată în cadrul reuniunii, precum şi alte documente ce se referă la ea pot fi transmise la adresa participanţilor, la indicaţia conducătorului care a permis desfăşurarea reuniunii, conform listei de expediere aprobate de către acesta. Dacă documentele în cauză se transmit numai pentru informare, atunci ele trebuie restituite în termenul fixat.

767. Caietele de lucru, predate Subdiviziunii de protecţie la finele reuniunii, se transmit la adresa participanţilor sau se distrug, în modul stabilit de prezentul Regulament.

768. La încheierea lucrărilor, persoana responsabilă de organizarea reuniunii va inspecta încăperea unde aceasta s-a desfăşurat, pentru a asigura colectarea tuturor materialelor utilizate la reuniune şi a exclude orice posibilitate de acces neautorizat la informaţiile atribuite la secret de stat.

Capitolul IX

MĂSURI DE PROTECŢIE FIZICĂ A SECRETULUI DE STAT

769. Obiectivele, sectoarele şi locurile în care sînt gestionate informaţiile atribuite la secret de stat trebuie protejate fizic împotriva accesului neautorizat.

770. Măsurile de protecţie fizică – grilaje la ferestre, încuietori la uşi, pază la intrări, sisteme automate pentru supraveghere, control, acces, patrule de pază, dispozitive de alarmă, mijloace pentru detectarea observării, ascultării sau interceptării, vor fi stabilite în raport cu:

1) gradul de secretizare a informaţiilor, volumul şi localizarea acestora;

2) tipul safeurilor, dulapurilor de metal, ambalajelor şi altor suporţi în care sînt păstrate (depozitate) informaţiile;

3) locul de amplasare a spaţiilor/locurilor unde se păstrează sau se concentrează informaţiile atribuite la secret de stat ori se desfăşoară astfel de activităţi;

4) caracteristicile clădirii şi zonei de amplasare.

771. Zonele în care sînt manipulate sau stocate informaţiile atribuite la secret de stat trebuie organizate şi administrate în aşa fel încît să corespundă uneia dintre următoarele categorii:

1) zonă de securitate clasa I, care presupune că orice persoană aflată în interiorul acesteia are acces la informaţii atribuite la secret de stat de gradul „Strict secret" şi „Secret" şi care necesită:

a) perimetru clar delimitat şi protejat, în care toate intrările şi ieşirile sînt supravegheate;

b) controlul sistemului de intrare, care să permită numai accesul persoanelor verificate corespunzător şi autorizate în mod special;

c) indicarea gradului de secretizare a informaţiilor existente în zonă;

2) zonă de securitate clasa a II-a, care presupune gestionarea informaţiilor cu gradul de secretizare „Confidenţial" şi „Restricţionat" şi se realizează prin aplicarea unor măsuri specifice de protecţie împotriva accesului persoanelor neautorizate şi care necesită:

a) perimetru clar delimitat şi protejat, în care toate intrările şi ieşirile sînt supravegheate;

b) controlul sistemului de intrare care să permită accesul neînsoţit numai persoanelor verificate şi autorizate să pătrundă în această zonă;

c) reguli de însoţire, supraveghere şi prevenire a accesului persoanelor neautorizate la informaţiile atribuite la secret de stat.

772. Încăperile în care nu se lucrează zilnic 24 de ore vor fi inspectate imediat după terminarea programului de lucru, pentru a verifica dacă informaţiile atribuite la secret de stat sînt asigurate în mod corespunzător.

773. În jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilită o zonă administrativă, cu perimetru vizibil delimitat, în interiorul căreia să existe posibilitatea de control al personalului şi al vehiculelor.

774. Accesul în zonele de securitate clasa I şi clasa a II-a va fi controlat prin verificarea permisului de acces sau printr-un sistem de recunoaştere individuală aplicat personalului.

775. Autorităţile publice sau alte persoane juridice deţinătoare de informaţii atribuite la secret de stat vor institui un sistem propriu de control al vizitatorilor, destinat interzicerii accesului neautorizat al acestora în zonele de securitate.

776. Permisul de acces nu va specifica, în clar, identitatea autorităţii publice sau al altei persoane juridice ori locul în care deţinătorul are acces.

777. Autorităţile publice sau alte persoane juridice vor organiza, la intrarea sau la ieşirea din zonele de securitate clasa I sau clasa a II-a, controale planificate şi inopinate ale bagajelor, incluzînd colete, genţi şi alte tipuri de suporţi în care s-ar putea transporta materiale şi informaţii atribuite la secret de stat.

778. Personalul inclus în sistemul de pază şi apărare a obiectivelor, sectoarelor şi locurilor în care sînt gestionate informaţii atribuite la secret de stat trebuie să deţină autorizaţie de acces de forma corespunzătoare gradului de secretizare a informaţiilor necesare îndeplinirii atribuţiilor ce îi revin.

779. Este interzis accesul necontrolat cu aparate de fotografiat, filmat, înregistrare audio-video, de copiat din baze de date informatice sau de comunicare la distanţă în locurile în care se află informaţii atribuite la secret de

stat. Regulamentul privind accesul cu aparate de fotografiat, filmat, înregistrare audio-video, de copiat din bazele de date informatice sau de comunicare la distanţă în locurile în care se află informaţii atribuite la secret de stat se aprobă de către conducătorul autorităţii publice sau al altei persoane juridice respective.

780. Conducătorii autorităţilor publice sau ai altor persoane juridice deţinătoare de informaţii atribuite la secret de stat vor stabili reguli cu privire la circulaţia şi ordinea interioară în zonele de securitate, astfel încît accesul să fie permis exclusiv titularilor de autorizaţii de acces, cu respectarea principiului necesităţii de a lucra cu informaţii atribuite la secret de stat.

781. Accesul pentru intervenţii tehnice, reparaţii sau activităţi de deservire în locurile în care se lucrează cu informaţii atribuite la secret de stat ori în care se păstrează, se prelucrează sau se multiplică astfel de informaţii este permis numai angajaţilor autorităţii publice sau ai altei persoane juridice, care deţin autorizaţii de acces de forma corespunzătoare celui mai înalt grad de secretizare a informaţiilor pe care le-ar putea cunoaşte.

782. Pentru a distinge persoanele care au acces în diferite locuri sau sectoare în care sînt gestionate informaţii atribuite la secret de stat, acestea pot purta însemne sau echipamente specifice.

783. În locurile şi sectoarele în care sînt gestionate informaţii atribuite la secret de stat, însemnele şi echipamentele distinctive se stabilesc prin regulamente de ordine interioară.

784. Evidenţa legitimaţiilor, permiselor şi a altor însemne şi echipamente distinctive se ţine de Subdiviziunea de protecţie a autorităţii publice sau a altei persoane juridice.

785. Persoanele care pierd permisele de acces, însemnele sau echipamentele specifice sînt obligate să anunţe imediat şeful ierarhic superior şi subdiviziunea de protecţie. Concomitent, faptul pierderii se aduce la cunoştinţa conducătorului autorităţii publice sau al altei persoane juridice.

786. În situaţiile menţionate în punctul 785 din prezentul Regulament, conducătorul autorităţii publice sau al altei persoane juridice va dispune investigarea împrejurărilor în care s-au produs şi va informa Serviciul de Informaţii şi Securitate.

787. Subdiviziunea de protecţie trebuie să întreprindă măsurile ce se impun pentru a preveni folosirea permiselor de acces, însemnelor sau echipamentelor specifice de către persoane neautorizate.

788. Accesul fiecărui angajat al autorităţii publice sau al altei persoane juridice deţinătoare de informaţii atribuite la secret de stat în zone de securitate clasa I sau clasa a II-a se realizează prin intrări anume stabilite, pe baza permisului de acces, semnat de conducătorul acesteia.

789. Permisele de acces vor fi individuale, prin aplicarea unor semne distinctive.

790. La încetarea activităţii, permisele de acces se retrag şi se anulează.

791. În locurile în care sînt gestionate informaţii atribuite la secret de stat este interzis accesul altor persoane, în afara celor care dispun de permis de acces.

792. Accesul persoanelor din afara autorităţii publice sau al altei persoane juridice în zona administrativă sau în zonele de securitate este permis numai dacă sînt însoţite de persoane anume desemnate, cu bilet de intrare eliberat pe baza documentelor de legitimare, de către conducătorul autorităţii publice sau al altei persoane juridice.

793. Accesul angajaţilor persoanelor juridice care efectuează lucrări de construcţii, reparaţii şi întreţinere a clădirilor, instalaţiilor sau utilităţilor în zonele administrative ori în zonele de securitate se realizează cu documente de acces temporar, eliberate de conducătorii autorităţilor publice sau ai altor persoane juridice beneficiare, pe baza actelor de identitate, la solicitarea reprezentanţilor autorizaţi ai persoanelor juridice în cauză.

794. Locurile în care se efectuează lucrările menţionate se supraveghează de către persoane anume desemnate din autoritatea publică sau altă persoană juridică beneficiară.

795. Documentul de acces temporar este valabil pe durata executării lucrărilor, iar la finisarea activităţilor se restituie emitentului.

796. Pierderea documentului de acces temporar va fi luată în evidenţa Subdiviziunii de protecţie, care va dispune măsurile necesare de prevenire a folosirii lui de către persoane neautorizate.

797. Reprezentanţii organului abilitat – Serviciul de Informaţii şi Securitate, pot să efectueze controlul privind starea protecţiei secretului de stat în cadrul autorităţilor publice şi al altor persoane juridice ce au acces la obiectivele, sectoarele şi locurile în care sînt gestionate informaţii atribuite la secret de stat, pe baza legitimaţiei de serviciu şi a delegaţiei speciale, semnate de conducătorul organului pe care-l reprezintă.

798. Persoanele aflate la practică, stagii de instruire sau schimb de experienţă au acces numai în locurile stabilite de conducătorul autorităţii publice sau al altei persoane juridice, pe baza permiselor de acces eliberate în acest sens.

799. Persoanele care solicită angajări, audienţe ori care prezintă reclamaţii şi sesizări vor fi primite în afara zonelor administrative sau în locuri special amenajate, cu aprobarea conducătorului autorităţii publice sau al altei persoane juridice.

800. În caz de necesitate, la decizia conducătorului autorităţii publice sau al altei persoane juridice respective, în afara orelor de program şi în zilele nelucrătoare se vor organiza patrulări pe perimetrul autorităţii publice sau al altei persoane juridice, la intervale care vor fi stabilite prin instrucţiuni elaborate

în baza planului de pază şi apărare a obiectivului.

801. Sistemele de pază, supraveghere şi control-acces trebuie să asigure prevenirea pătrunderii neautorizate în obiectivele, sectoarele şi locurile unde sînt gestionate informaţii atribuite la secret de stat.

802. Timpul de reacţie a personalului de pază şi apărare va fi testat periodic, pentru a garanta intervenţia operativă în situaţii de urgenţă.

803. Autorităţile publice sau alte persoane juridice trebuie să întocmească şi să aprobe Programul propriu de prevenire a scurgerii de informaţii atribuite la secret de stat, conform formei nr. 73, anexă la prezentul Regulament, şi să asigure aplicarea acestuia. Programul de prevenire a scurgerii de informaţii atribuite la secret de stat se avizează de Serviciul de Informaţii şi Securitate. De asemenea, autorităţile publice sau alte persoane juridice care gestionează informaţii atribuite la secret de stat vor întocmi planul de pază şi apărare a obiectivelor, sectoarelor şi locurilor care prezintă importanţă deosebită pentru protecţia informaţiilor atribuite la secret de stat.

804. Planul de pază şi apărare menţionat va fi înregistrat potrivit celui mai înalt grad de secretizare a informaţiilor protejate şi va cuprinde totalitatea măsurilor de securitate luate pentru prevenirea accesului neautorizat la acestea.

805. Planul de pază şi apărare va fi anexat Programului de prevenire a scurgerii de informaţii atribuite la secret de stat şi va cuprinde:

1) date privind delimitarea şi marcarea zonelor de securitate, dispunerea posturilor de pază şi măsurile de supraveghere a perimetrului protejat;

2) sistemul de control al accesului în zonele de securitate;

3) măsurile de avertizare şi alarmare pentru situaţii de urgenţă;

4) planul de evacuare a documentelor şi modul de acţiune în caz de urgenţă;

5) procedura de raportare, investigare şi evidenţă a încălcărilor reglementărilor privind protecţia informaţiilor atribuite la secret de stat.

806. Informaţiile atribuite la secret de stat se păstrează în safeuri, dulapuri de metal, ambalaje şi alţi suporţi speciali, clasificate conform următoarelor clase:

1) clasa A – autorizate la nivel naţional pentru păstrarea informaţiilor secretizate cu parafa „Strict secret” în zona de securitate clasa I;

2) clasa B – autorizate la nivel naţional pentru păstrarea informaţiilor avînd gradele de secretizare „Secret”, „Confidenţial” şi „Restricţionat” în zone de securitate clasa I sau clasa a II-a;

3) clasa C – mobilier de birou adecvat numai pentru păstrarea informaţiilor secretizate cu parafa „Restricţionat”.

807. Evidenţa safeurilor, dulapurilor de metal, ambalajelor şi altor suporţi speciali,

precum şi a cheilor de la acestea se ţine de către Subdiviziunea de protecţie într-un registru special, potrivit formei nr. 74, anexă la prezentul Regulament.

808. Safeurile, dulapurile de metal, ambalajele şi alţi suporţi speciali din clasele A şi B vor fi construite astfel încît să asigure protecţia împotriva pătrunderii clandestine şi deteriorării sub orice formă a informaţiilor.

809. Cerinţele la care trebuie să corespundă safeurile, dulapurile de metal, ambalajele şi alţi suporţi speciali din clasele A şi B se elaborează, în conformitate cu standardele naţionale şi internaţionale în vigoare, de către Comisia interdepartamentală pentru protecţia secretului de stat în colaborare cu autorităţile administraţiei publice competente.

810. Încăperile de securitate sînt încăperile special amenajate în zone de securitate clasa I sau clasa a II-a, în care informaţiile atribuite la secret de stat pot fi păstrate pe rafturi deschise sau pot fi expuse pe hărţi, planşe ori diagrame.

811. Pereţii, podelele, plafoanele, uşile şi încuietorile încăperilor de securitate vor asigura protecţia echivalentă clasei safeurilor, dulapurilor de metal, ambalajelor şi altor suporţi de securitate aprobate pentru păstrarea informaţiilor atribuite la secret de stat, corespunzător gradului de secretizare.

812. Ferestrele încăperilor de securitate dispuse la parter sau ultimul etaj vor fi protejate obligatoriu cu gratii fixate în beton sau asigurate antiefracţie.

813. În afara programului de lucru, uşile încăperilor de securitate vor fi sigilate, iar sistemul de ventilare asigurat împotriva accesului neautorizat şi introducerii materialelor incendiare.

814. În situaţii de urgenţă, dacă informaţiile atribuite la secret de stat trebuie evacuate, se vor utiliza ambalaje speciale autorizate la nivel naţional, din clasa corespunzătoare gradului de secretizare a acestor informaţii.

815. Încuietorile folosite la safeurile, dulapurile de metal, ambalajele, alţi suporţi speciali şi încăperile de securitate în care sînt păstrate informaţii atribuite la secret de stat se împart în trei grupe, astfel:

1) grupa A – încuietori autorizate pentru safeurile, dulapurile de metal, ambalajele, alţi suporţi speciali din clasa A;

2) grupa B – încuietori autorizate pentru safeurile, dulapurile de metal, ambalajele, alţi suporţi speciali din clasa B;

3) grupa C – încuietori pentru mobilierul de birou (clasa C).

816. Cerinţele cărora trebuie să corespundă mecanismele de închidere, sistemele cu cifru şi încuietorile, pe grupe de utilizare, se elaborează, în conformitate cu standardele naţionale şi internaţionale în vigoare, de către Comisia interdepartamentală pentru protecţia secretului de stat în colaborare cu autorităţile administraţiei publice competente.

817. Cheile safeurilor, dulapurilor de metal, ambalajelor, altor suporţi speciali de securitate şi încăperilor de securitate, conform listei aprobate de către conducătorul autorităţii publice sau al altei persoane juridice respective, nu vor fi scoase din zonele de securitate.

818. În afara orelor de program, cheile de la încăperile, safeurile, dulapurile de metal, ambalajele, alţi suporţi speciali de securitate, conform listei aprobate de către conducătorul autorităţii publice sau al altei persoane juridice respective, se păstrează în cutii sigilate de către personalul care asigură paza şi apărarea.

819. Predarea şi primirea cheilor de la încăperile, safeurile, dulapurile de metal, ambalajele, alţi suporţi speciali de securitate se face, pe bază de semnătură (recipisă), într-un borderou special destinat, conform formei nr. 75, anexă la prezentul Regulament.

820. Pentru situaţiile de urgenţă, un rînd de chei suplimentare sau, după caz, o evidenţă scrisă a combinaţiilor încuietorilor vor fi păstrate în plicuri opace sigilate, în ambalaje separate, într-o subdiviziune stabilită de conducerea autorităţii publice sau a altei persoane juridice, sub control corespunzător.

821. Evidenţa fiecărei combinaţii se va păstra în plic separat.

822. Cheilor şi plicurilor cu combinaţii trebuie să li se asigure gradul de protecţie necesar, în baza deciziei conducătorului autorităţii publice sau al altei persoane juridice respective, acelaşi grad de protecţie ca şi informaţiilor la care permit accesul.

823. Combinaţiile încuietorilor de la încăperile, safeurile, dulapurile de metal, ambalajele şi alţi suporţi de securitate vor fi cunoscute de un număr restrîns de persoane desemnate de conducerea autorităţii publice sau a altei persoane juridice.

824. Cheile şi combinaţiile încuietorilor vor fi schimbate:

1) ori de cîte ori are loc o schimbare de personal;

2) de fiecare dată cînd se constată că au intervenit situaţii de natură să le facă vulnerabile;

3) la intervale regulate, de preferinţă o dată la şase luni, fără a se depăşi 12 luni.

Cheile şi combinaţiile încuietorilor vor fi schimbate de fiecare dată cînd se constată că au intervenit situaţii de natură să le facă vulnerabile. Combinaţiile încuietorilor vor fi schimbate la intervale regulate, de preferinţă o dată la şase luni, fără a se depăşi 12 luni, şi în caz de schimbare a personalului.

825. Sistemele electronice de alarmare sau de supraveghere destinate protecţiei informaţiilor atribuite la secret de stat vor fi prevăzute cu surse de alimentare de rezervă.

826. Orice defecţiune sau intervenţie neautorizată asupra sistemelor de alarmă sau de supraveghere destinate protecţiei informaţiilor atribuite la secret de stat trebuie să avertizeze personalul care le monitorizează.

827. Dispozitivele de alarmare trebuie să intre în funcţiune în cazul penetrării pereţilor, podelelor, tavanelor şi deschizăturilor sau la mişcări în interiorul încăperilor de securitate.

828. Copiatoarele şi dispozitivele telefax se vor instala în încăperi special destinate şi se vor folosi numai de către persoanele autorizate, potrivit gradului de secretizare a informaţiilor la care au acces.

829. Autorităţile publice sau alte persoane juridice deţinătoare de informaţii atribuite la secret de stat au obligaţia de a asigura protecţia acestora împotriva ascultărilor neautorizate, pasive sau active.

830. Protecţia împotriva ascultării pasive a discuţiilor secrete se realizează prin izolarea fonică a încăperilor.

831. Protecţia împotriva ascultărilor active, prin microfoane, radio-emiţători şi alte dispozitive implantate, se realizează pe baza inspecţiilor de securitate a încăperilor, accesoriilor, instalaţiilor, sistemelor de comunicaţii, echipamentelor şi mobilierului de birou, precum şi prin efectuarea măsurilor speciale tehnice (inclusiv utilizarea aparatajului special de protecţie a convorbirilor), realizate de instituţii specializate, potrivit competenţelor legale.

832. Lista încăperilor protejate împotriva ascultărilor trebuie să fie aprobată de către conducătorul autorităţii publice sau al altei persoane juridice respective. Accesul în încăperile protejate împotriva ascultărilor se va controla în mod special.

833. Periodic, personalul specializat în depistarea dispozitivelor de ascultare va efectua inspecţii fizice şi tehnice.

834. Inspecţiile fizice şi tehnice se organizează, în mod obligatoriu, în urma oricărei intrări neautorizate sau suspiciuni privind accesul persoanelor neautorizate şi după executarea lucrărilor de reparaţii, întreţinere, zugrăvire sau redecorare.

835. Nici un obiect nu va fi introdus în încăperile protejate împotriva ascultării, fără a fi verificat în prealabil de către personalul specializat în depistarea dispozitivelor de ascultare.

836. În zonele în care se poartă discuţii secrete şi care sînt asigurate din punct de vedere tehnic nu se vor instala telefoane, iar dacă instalarea acestora este absolut necesară, acestea trebuie prevăzute cu un dispozitiv de deconectare pasiv. Inspecţiile de securitate tehnică în aceste zone trebuie efectuate, în mod obligatoriu, înaintea începerii convorbirilor, pentru identificarea fizică a dispozitivelor de ascultare şi verificarea sistemelor telefonice, electrice sau de

altă natură, care ar putea fi utilizate ca mediu de atac.

837. Echipamentele de comunicaţii şi dotările din birouri, în principal cele electrice şi electronice, trebuie verificate de specialişti ai organului competent pentru protecţia secretului de stat, înainte de a fi folosite în zonele în care se lucrează ori se discută despre informaţii avînd gradele de secretizare „Strict secret" sau „Secret", pentru a preveni transmiterea sau interceptarea, în afara cadrului legal, a unor informaţii inteligibile. Pentru aceste zone, la decizia conducătorului autorităţii publice sau al altei persoane juridice respective, se va organiza o evidenţă a tipului şi numerelor de inventar ale echipamentului şi mobilei mutate în/din interiorul încăperilor, care va fi gestionată ca material secret de stat.

Capitolul X

MĂSURI DE PROTECŢIE TEHNICĂ ŞI CRIPTOGRAFICĂ A SECRETULUI DE STAT

Secţiunea 1

Dispoziţii generale

838. Modalităţile şi măsurile de protecţie a informaţiilor atribuite la secret de stat, care se prezintă în format electronic, sînt similare celor pe suport de hîrtie.

839. În sensul prezentului capitol se definesc următoarele noţiuni şi abrevieri:

1) INFOSEC – ansamblul măsurilor şi structurilor de protecţie a informaţiilor atribuite la secret de stat, care sînt prelucrate, păstrate sau transmise prin intermediul sistemelor de comunicaţii electronice, împotriva ameninţărilor şi a oricăror acţiuni care pot aduce atingere confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi nerepudierii informaţiilor atribuite la secret de stat, precum şi afectarea funcţionării sistemelor electronice, indiferent dacă acestea apar accidental sau intenţionat. Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum şi depistarea şi prevenirea ameninţărilor la care sînt expuse informaţiile şi sistemele;

2) informaţii în format electronic – texte, date, imagini, sunete, înregistrate pe dispozitive de stocare sau pe suporţi magnetici, optici, electrici ori transmise sub formă de curenţi, tensiuni sau cîmp electromagnetic, în eter sau în reţele de comunicaţii;

3) sistem de prelucrare automată a datelor (SPAD) – ansamblul de elemente interdependente în care se includ: echipamentele de calcul, produsele software de bază şi aplicative, metodele, procedeele şi, dacă este cazul, personalul, organizate astfel încît să asigure îndeplinirea funcţiilor de stocare, prelucrare automată şi transmitere a informaţiilor în format electronic şi care se află sub coordonarea şi controlul unei singure autorităţi. Un SPAD poate să cuprindă

subsisteme, iar unele dintre acestea pot fi ele însele SPAD;

4) componente specifice de securitate ale unui SPAD – ansamblul de elemente necesare asigurării unui nivel corespunzător de protecţie pentru informaţiile atribuite la secret de stat, care urmează a fi stocate sau procesate într-un SPAD. Acestea sînt:

a) funcţii şi caracteristici hardware/firmware/software;

b) proceduri de operare şi moduri de operare;

c) proceduri de evidenţă;

d) controlul accesului;

e) definirea zonei de operare a SPAD;

f) definirea zonei de operare a posturilor de lucru/a terminalelor la distanţă;

g) restricţii impuse de politica de management;

h) structuri fizice şi dispozitive;

i) mijloace de control pentru personal şi comunicaţii;

j) reţele de transmisii de date (RTD);

5) reţele de transmisii de date (RTD) – ansamblul de elemente interdependente în care se includ: echipamente, programe şi dispozitive de comunicaţie, tehnică de calcul hardware şi software, metode şi proceduri pentru transmisie şi recepţie de date şi controlul reţelei, precum şi, dacă este cazul, personalul aferent. Toate acestea sînt organizate astfel încît să asigure îndeplinirea funcţiilor de transmisie a informaţiilor în format electronic între două sau mai multe SPAD sau să permită interconectarea cu alte RTD-uri. O RTD poate utiliza serviciile unuia sau mai multor sisteme de comunicaţii; mai multe RTD pot utiliza serviciile unuia şi aceluiaşi sistem de comunicaţii. Caracteristicile de securitate ale unei RTD cuprind: caracteristicile de securitate ale sistemelor SPAD individuale conectate, împreună cu toate componentele şi facilităţile asociate reţelei – facilităţi de comunicaţii ale reţelei, mecanisme şi proceduri de identificare şi etichetare, controlul accesului, programe şi proceduri de control şi revizie, necesare pentru asigurarea unui nivel corespunzător de protecţie a informaţiilor atribuite la secret de stat, care sînt transmise prin intermediul RTD;

6) RTD locală – reţea de transmisii de date care interconectează mai multe computere sau echipamente de reţea, situate în acelaşi perimetru;

7) sistem informatic şi de comunicaţii (SIC) – ansamblu informatic prin intermediul căruia se stochează, se procesează şi se transmit informaţii în format electronic, alcătuit din cel puţin un SPAD, izolat sau conectat la o RTD. SIC poate avea o configuraţie complexă, formată din mai multe SPAD-uri şi/sau RTD-uri interconectate;

8) securitatea SPAD, RTD şi SIC – aplicarea măsurilor de securitate la SPAD, RTD şi SIC cu scopul de a preveni sau împiedica extragerea sau modificarea informaţiilor atribuite la secret de stat stocate, procesate, transmise prin intermediul acestora – prin interceptare, alterare, distrugere, accesare neautorizată cu mijloace electronice, precum şi invalidarea de servicii sau funcţii, prin mijloace specifice;

9) confidenţialitate – proprietatea informaţiei din cadrul sistemului care caracterizează protecţia ei de la accesul neautorizat (asigurarea accesului la informaţii atribuite la secret de stat a persoanei numai în baza autorizaţiei de acces de forma corespunzătoare gradului de secretizare a informaţiei accesate şi în baza principiului necesităţii de a lucra cu asemenea informaţii);

10) integritate – proprietatea informaţiei din cadrul sistemului, care caracterizează veridicitatea, concordanţa şi invariabilitatea acesteia, inclusiv în condiţiile de acţiune intenţionată sau neintenţionată cu scopul modificării sau distrugerii acesteia, precum şi interdicţia modificării prin ştergere sau adăugare ori a distrugerii în mod neautorizat a informaţiilor atribuite la secret de stat;

11) accesibilitate – proprietatea informaţiei din cadrul sistemului, care caracterizează posibilitatea accesării libere a informaţiei pentru efectuarea operaţiunilor sancţionate, precum şi asigurarea condiţiilor necesare regăsirii şi utilizării cu uşurinţă, ori de cîte ori este nevoie, cu respectarea strictă a condiţiilor de confidenţialitate şi integritate a informaţiilor atribuite la secret de stat;

12) autenticitate – asigurarea posibilităţii de verificare a identităţii pe care un utilizator de SPAD sau RTD pretinde că o are;

13) nerepudiere – măsură prin care se asigură faptul că, după emiterea/recepţionarea unei informaţii într-un sistem de comunicaţii securizat, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informaţii;

14) risc de securitate – probabilitatea ca o ameninţare sau o vulnerabilitate a SPAD sau RTD – SIC să se materializeze în mod efectiv;

15) management de risc – activitatea de identificare, control şi minimizare a riscurilor de securitate, fiind una continuă de stabilire şi menţinere a unui nivel de securitate în domeniul tehnologiei informaţiei şi comunicaţiilor – într-o autoritate publică sau altă persoană juridică, în sensul că, pornind de la analiza de risc, identifică şi evaluează ameninţările şi vulnerabilităţile şi propune aplicarea măsurilor adecvate de contracarare, proiectate la un preţ de cost corelat cu consecinţele care ar decurge din divulgarea, modificarea sau ştergerea informaţiilor care trebuie protejate;

16) regula celor doi – obligativitatea colaborării a două persoane pentru îndeplinirea unei activităţi specifice;

17) produs informatic de securitate – componentă de securitate care se încorporează într-un SPAD sau RTD – SIC şi care serveşte la sporirea

sau asigurarea confidenţialităţii, integrităţii, accesibilităţii, autenticităţii şi nerepudierii informaţiilor stocate, procesate sau transmise;

18) securitatea calculatoarelor (COMPUSEC) – aplicarea la nivelul fiecărui calculator a facilităţilor de securitate hardware, software şi firmware, pentru a preveni divulgarea, utilizarea, modificarea sau ştergerea neautorizată a informaţiilor atribuite la secret de stat ori invalidarea neautorizată a unor funcţii;

19) securitatea comunicaţiilor (COMSEC) – aplicarea măsurilor de securitate în telecomunicaţii, cu scopul de a proteja mesajele dintr-un sistem de telecomunicaţii, care ar putea fi interceptate, studiate, analizate şi, prin reconstituire, pot conduce la divulgarea informaţiilor atribuite la secret de stat. COMSEC reprezintă ansamblul de proceduri, incluzînd:

a) măsuri de securitate a transmisiilor;

b) măsuri de securitate împotriva radiaţiilor – TEMPEST;

c) măsuri de acoperire criptologică;

d) măsuri de securitate fizică, procedurală, de personal şi a documentelor;

e) măsuri COMPUSEC;

20) TEMPEST – ansamblul măsurilor de testare şi de realizare a securităţii împotriva scurgerii de informaţii, prin intermediul emisiilor electromagnetice parazite;

21) evaluare – examinarea detaliată, din punct de vedere tehnic şi funcţional, a aspectelor de securitate ale SPAD şi RTD – SIC sau a produselor de securitate, de către organul abilitat în acest sens. În procesul de evaluare se verifică:

a) prezenţa facilităţilor/funcţiilor de securitate cerute;

b) absenţa efectelor secundare compromiţătoare care ar putea decurge din implementarea facilităţilor de securitate;

c) funcţionalitatea globală a sistemului de securitate;

d) satisfacerea cerinţelor de securitate specifice pentru un SPAD şi RTD – SIC;

e) stabilirea nivelului de încredere al SPAD sau RTD – SIC ori al produselor informatice de securitate implementate;

f) existenţa performanţelor de securitate ale produselor informatice de securitate instalate în SPAD sau RTD – SIC;

22) certificare – emiterea unui document în baza unei evaluări care atestă nivelul de corespundere a mijloacelor de protejare a informaţiilor atribuite la secret de stat cu cerinţele de protecţie a informaţiilor avînd gradul corespunzător de secretizare (măsura în care SPAD şi RTD – SIC satisfac cerinţele de securitate,

precum şi măsura în care produsele informatice de securitate corespund exigenţelor referitoare la protecţia informaţiilor atribuite la secret de stat);

23) zona SPAD – zona de lucru în care se găsesc şi operează unul sau mai multe calculatoare, unităţi periferice locale şi de stocare, mijloace de control şi echipament specific de reţea şi de comunicaţii. Zona SPAD nu include zona în care sînt amplasate terminale, echipamente periferice sau staţii de lucru la distanţă, chiar dacă aceste echipamente sînt conectate la echipamentul central de calcul din zona SPAD;

24) zona terminal/staţie de lucru la distanţă – zona separată de zona SPAD în care se găsesc:

a) elemente de tehnică de calcul;

b) echipamentele periferice locale, terminale sau staţii de lucru la distanţă, conectate la echipamentele din zona SPAD;

c) echipamente de comunicaţii;

25) ameninţare – posibilitatea de compromitere accidentală sau deliberată a securităţii SPAD sau RTD -SIC, prin pierderea confidenţialităţii, a integrităţii sau disponibilităţii informaţiilor în format electronic sau prin afectarea funcţiilor care asigură autenticitatea şi nerepudierea informaţiilor;

26) vulnerabilitate – slăbiciune sau lipsă de control care ar putea permite sau facilita o manevră tehnică, procedurală sau operaţională, prin care se ameninţă o valoare sau ţintă specifică;

27) TIC – tehnologia informaţiei şi comunicaţiilor.

840. Informaţiile care se prezintă în format electronic pot fi:

1) stocate şi procesate în cadrul SPAD sau transmise prin intermediul RTD;

2) stocate şi transportate prin intermediul suporţilor de memorie, dispozitivelor electronice – cipuri de memorie, hîrtie perforată sau alţi suporţi specifici.

841. Încărcarea informaţiilor pe mediile prevăzute în punctul 840 subpunctul 2), precum şi interpretarea lor pentru a deveni inteligibile se face cu ajutorul echipamentelor electronice specializate.

842. Sistemele SPAD şi RTD – SIC au dreptul să stocheze, să proceseze sau să transmită informaţii atribuite la secret de stat, numai dacă sînt autorizate, conform prezentului Regulament.

843. În vederea autorizării SPAD şi RTD – SIC, autorităţile publice şi alte persoane juridice vor întocmi, cu aprobarea organelor lor de conducere, strategia proprie de securitate, în baza căreia vor implementa sisteme proprii de securitate, care vor include utilizarea de produse specifice tehnologiei informaţiei şi comunicaţiilor, personal instruit şi măsuri de protecţie a informaţiei, incluzînd

controlul accesului la sistemele şi serviciile informatice şi de comunicaţii, pe baza principiului necesităţii de a lucra cu informaţii atribuite la secret de stat şi al gradului de secretizare atribuit.

844. SPAD şi RTD – SIC vor fi supuse procesului de certificare, urmat de evaluări periodice.

845. Aplicarea reglementărilor în vigoare cu privire la protecţia informaţiilor atribuite la secret de stat în format electronic funcţionează unitar la nivel naţional. Sistemul de emitere şi implementare a măsurilor de securitate adresate protecţiei informaţiilor atribuite la secret de stat, care sînt stocate, procesate sau transmise de SPAD sau RTD – SIC, precum şi controlul modului de implementare a măsurilor de securitate se realizează de către organul desemnat la nivel naţional pentru protecţia secretului de stat.

846. Măsurile de protecţie a informaţiilor atribuite la secret de stat în format electronic trebuie reactualizate permanent, prin depistare, documentare şi gestionare a ameninţărilor şi vulnerabilităţilor la adresa informaţiilor atribuite la secret de stat şi a sistemelor care le prelucrează, le stochează şi le transmit.

847. Măsurile de securitate INFOSEC sînt structurate după gradul de secretizare a informaţiilor pe care le protejează şi în conformitate cu conţinutul acestora.

848. Conducătorul autorităţii publice sau al altei persoane juridice deţinătoare de informaţii atribuite la secret de stat răspunde de securitatea propriilor informaţii care sînt stocate, procesate sau transmise în SPAD sau RTD – SIC.

849. În fiecare autoritate publică sau altă persoană juridică care administrează SPAD şi RTD - SIC în care se stochează, se procesează sau se transmit informaţii atribuite la secret de stat se va institui o structură de securitate pentru tehnologia informaţiei şi a comunicaţiilor – SSTIC, în subordinea Subdiviziunii de protecţie.

850. În funcţie de volumul de activitate şi în cazul în care cerinţele de securitate permit, atribuţiile SSTIC pot fi îndeplinite numai de către un angajat de securitate TIC sau pot fi preluate, în totalitate, de către Subdiviziunea de protecţie.

851. SSTIC îndeplineşte atribuţii privind:

1) implementarea metodelor, mijloacelor şi măsurilor necesare protecţiei informaţiilor în format electronic;

2) exploatarea operaţională a SPAD şi RTD – SIC în condiţii de securitate;

3) coordonarea cooperării dintre autoritatea publică sau altă persoană juridică deţinătoare a SPAD sau RTD – SIC şi organul competent pentru protecţia secretului de stat;

4) implementarea măsurilor de securitate şi protecţie criptografică ale SPAD sau RTD – SIC.

852. SSTIC reprezintă punctul de contact între organul competent pentru protecţia secretului de stat şi autorităţile publice sau alte persoane juridice care deţin în administrare SPAD sau RTD – SIC şi, după caz, poate fi învestită, temporar, de către acesta, cu unele dintre atribuţiile sale.

853. Propunerile pe linie de securitate înaintate de către SSTIC devin aplicabile numai după ce sînt aprobate de către conducerea autorităţii publice sau al altei persoane juridice care deţine în administrare respectivul SPAD sau RTD – SIC.

854. SSTIC se instituie la nivelul fiecărei SPAD şi RTD – SIC şi reprezintă persoana sau subdiviziunea cu atribuţii de implementare a metodelor, mijloacelor şi măsurilor de securitate şi de exploatare a SPAD şi RTD – SIC în condiţii de securitate.

855. SSTIC este formată din administratori de securitate, după caz, alţi specialişti privind SPAD sau RTD – SIC şi condusă de către funcţionarul de securitate TIC. Toată structura SSTIC face parte din personalul autorităţii publice sau al altei persoane juridice care administrează SPAD sau RTD – SIC.

856. Exercitarea atribuţiilor SSTIC trebuie să cuprindă întregul ciclu de viaţă al SPAD sau RTD – SIC, începînd cu proiectarea, continuînd cu elaborarea paşapoartelor tehnice (specificaţiilor, sarcinilor tehnice), testarea instalării, certificarea, testarea periodică, exploatarea operaţională, modificarea şi încheind cu scoaterea din uz. În anumite situaţii, rolul SSTIC poate fi preluat de către alte subdiviziuni ale autorităţii publice sau al altei persoane juridice, în decursul ciclului de viaţă.

857. SSTIC mijloceşte cooperarea dintre conducerea autorităţii publice sau al altei persoane juridice căreia îi aparţine SPAD sau RTD – SIC şi organul competent pentru protecţia secretului de stat, atunci cînd autoritatea publică sau altă persoană juridică:

1) planifică dezvoltarea sau achiziţia de SPAD sau RTD;

2) propune schimbări ale unei configuraţii de sistem existente;

3) propune conectarea unui SPAD sau a unei RTD – SIC cu un alt SPAD sau RTD – SIC;

4) propune schimbări ale modului de operare de securitate al SPAD sau RTD - SIC;

5) propune schimbări în programele existente sau utilizarea de noi programe, pentru optimizarea securităţii SPAD sau RTD – SIC;

6) iniţiază proceduri de modificare a gradului de secretizare a SPAD şi RTD

– SIC care au fost deja certificate;

7) planifică sau propune întreprinderea oricărei alte activităţi referitoare la îmbunătăţirea securităţii SPAD sau RTD – SIC deja certificate.

858. SSTIC, cu aprobarea organului competent pentru protecţia secretului de stat, stabileşte standardele şi procedurile de securitate care trebuie respectate de către furnizorii de echipamente, pe parcursul dezvoltării, instalării şi testării SPAD şi RTD – SIC şi răspunde pentru justificarea, selectarea, implementarea şi controlul componentelor de securitate, care fac parte din SPAD şi RTD – SIC.

859. SSTIC stabileşte, pentru structurile de securitate şi management ale SPAD şi RTD – SIC, încă de la înfiinţare, responsabilităţile pe care le vor exercita pe tot ciclul de viaţă al SPAD şi RTD – SIC respective.

860. Activitatea INFOSEC din SPAD şi RTD – SIC, desfăşurată de către SSTIC, trebuie condusă şi coordonată de persoane care deţin autorizaţie de acces la secretul de stat de forma corespunzătoare, cu pregătire de specialitate în domeniul sistemelor TIC şi al securităţii acestora, precum şi experienţă de cel puţin 2 ani în domeniu.

861. Protecţia SPAD şi RTD – SIC din componenţa sistemelor de armament şi de detecţie se defineşte în contextul general al sistemelor din care acestea fac parte şi se realizează prin aplicarea prevederilor prezentului Regulament.

Secţiunea a 2-a

Măsuri, cerinţe şi moduri de operare

862. Măsurile de protecţie a informaţiilor atribuite la secret de stat în format electronic se aplică sistemelor SPAD şi RTD – SIC, care stochează, procesează sau transmit asemenea informaţii.

863. Autorităţile publice sau alte persoane juridice deţinătoare de informaţii atribuite la secret de stat au obligaţia să stabilească şi să implementeze un ansamblu de măsuri de securitate a sistemelor SPAD şi RTD – SIC – fizice, de personal, administrative, de tip TEMPEST şi criptografic.

864. Măsurile de securitate destinate protecţiei SPAD şi RTD – SIC trebuie să asigure controlul accesului pentru prevenirea sau detectarea divulgării neautorizate a informaţiilor. În procesul de certificare va stabili dacă aceste măsuri sînt corespunzătoare.

865. Cerinţele de securitate specifice (CSS) se stabilesc într-un document încheiat între organul competent pentru protecţia secretului de stat şi SSTIC, ce cuprinde principii şi măsuri de securitate care trebuie să stea la baza procesului de certificare a SPAD sau RTD – SIC.

866. CSS se elaborează pentru fiecare SPAD şi RTD – SIC care stochează, procesează sau transmite informaţii atribuite la secret de stat. Acestea sînt

stabilite de către SSTIC şi aprobate de către organul competent pentru protecţia secretului de stat.

867. CSS se formulează încă din faza de proiectare a SPAD sau RTD – SIC şi se dezvoltă pe tot ciclul de viaţă al sistemului.

868. CSS au la bază standardele naţionale de protecţie, parametrii esenţiali ai mediului operaţional, nivelul minim de autorizare a personalului, gradul de secretizare a informaţiilor gestionate şi modul de operare a sistemului care urmează să fie supus certificării.

869. SPAD şi RTD – SIC care stochează, procesează sau transmit informaţii atribuite la secret de stat vor fi certificate şi autorizate să opereze, pe anumite perioade de timp, în unul dintre următoarele moduri de operare:

1) specializat;

2) de nivel înalt;

3) multinivel.

870. În modul de operare specializat, toate persoanele cu drept de acces la SPAD sau la RTD trebuie să aibă autorizaţie de acces la secret de stat de forma corespunzătoare celui mai înalt grad de secretizare a informaţiilor stocate, procesate sau transmise prin aceste sisteme, iar necesitatea de a lucra cu informaţii atribuite la secret de stat pentru aceste persoane se stabileşte cu privire la toate informaţiile stocate, procesate sau transmise în cadrul SPAD sau RTD – SIC.

871. În acest mod de operare, principiul necesităţii de a lucra cu informaţii atribuite la secret de stat nu impune o separare a informaţiilor în cadrul SPAD sau RTD, ca mijloc de securitate a SIC. Celelalte măsuri de protecţie prevăzute trebuie să asigure îndeplinirea cerinţelor impuse de cel mai înalt grad de secretizare a informaţiilor stocate, procesate sau transmise în cadrul SPAD sau RTD.

872. În modul de operare de nivel înalt, toate persoanele cu drept de acces la SPAD sau la RTD – SIC trebuie să aibă autorizaţie de acces la secret de stat de forma corespunzătoare celui mai înalt grad de secretizare a informaţiilor stocate, procesate sau transmise în cadrul SPAD sau RTD – SIC, iar accesul la informaţii se face diferenţiat, conform principiului necesităţii de a lucra cu informaţii atribuite la secret de stat.

873. Pentru a asigura accesul diferenţiat la informaţii, conform principiului necesităţii de a lucra cu informaţii atribuite la secret de stat, se instituie facilităţi de securitate care să asigure un acces selectiv şi separarea informaţiilor în cadrul SPAD sau RTD – SIC. Celelalte măsuri de protecţie trebuie să satisfacă cerinţele pentru cel mai înalt grad de secretizare a informaţiilor stocate, procesate, transmise în cadrul SPAD sau RTD – SIC.

874. Toate informaţiile stocate, procesate sau vehiculate în cadrul unui SPAD sau RTD – SIC în acest mod de operare vor fi protejate ca informaţii, avînd cel mai înalt grad de secretizare care a fost constatat în mulţimea informaţiilor stocate, procesate sau vehiculate prin sistem.

875. În modul de operare multinivel, accesul la informaţiile atribuite la secret de stat se face diferenţiat, potrivit principiului necesităţii de a lucra cu informaţii atribuite la secret de stat, conform următoarelor reguli:

1) nu toate persoanele cu drept de acces la SPAD sau RTD – SIC au autorizaţie de acces de forma corespunzătoare celui mai înalt grad de secretizare a informaţiilor care sînt stocate, procesate sau transmise prin aceste sisteme;

2) nu toate persoanele cu acces la SPAD sau RTD – SIC au acces la toate informaţiile stocate, procesate sau transmise prin aceste sisteme, accesul acordîndu-se diferenţiat, conform principiului necesităţii de a lucra cu informaţii atribuite la secret de stat.

876. Aplicarea regulilor prevăzute în punctul 875 din prezentul Regulament impune instituirea unor facilităţi de securitate care să asigure un mod selectiv şi individual de acces la informaţiile atribuite la secret de stat din cadrul SPAD sau RTD –SIC.

877. Securitatea SPAD, a reţelei şi a obiectivului SIC se asigură prin funcţiile de administrator de securitate.

878. Administratorii de securitate sînt:

1) administratorul de securitate al SPAD;

2) administratorul de securitate al reţelei;

3) administratorul de securitate al obiectivului SIC.

879. Funcţiile de administratori de securitate trebuie să asigure îndeplinirea atribuţiilor SSTIC. Dacă este cazul, aceste funcţii pot fi cumulate de către un singur specialist.

880. SSTIC desemnează un administrator de securitate al SPAD responsabil de supervizarea dezvoltării, implementării şi administrării măsurilor de securitate dintr-un SPAD, inclusiv participarea la elaborarea procedurilor operaţionale de securitate.

881. La recomandarea organului competent pentru protecţia secretului de stat, SSTIC poate desemna structuri de administrare ale SPAD, care îndeplinesc aceleaşi atribuţii.

882. Administratorul de securitate al reţelei este desemnat de SSTIC pentru un SIC de mari dimensiuni sau în cazul interconectării mai multor SPAD şi îndeplineşte atribuţii privind managementul securităţii comunicaţiilor.

883. Administratorul de securitate al obiectivului SIC este desemnat de SSTIC sau de organul competent pentru protecţia secretului de stat şi răspunde de asigurarea implementării şi menţinerea măsurilor de securitate aplicabile obiectivului SIC respectiv.

884. Responsabilităţile unui administrator de securitate al obiectivului SIC pot fi îndeplinite de către Subdiviziunea de protecţie a autorităţii publice sau al altei persoane juridice, ca parte a atribuţiilor sale de serviciu.

885. Obiectivul SIC reprezintă un amplasament specific sau un grup de amplasamente în care funcţionează un SPAD şi/sau RTD. Responsabilităţile şi măsurile de securitate pentru fiecare zonă de amplasare a unui terminal/staţie de lucru care funcţionează la distanţă trebuie să fie clar determinate.

886. Toţi utilizatorii de SPAD sau RTD – SIC poartă responsabilitatea în ceea ce priveşte securitatea acestor sisteme raportate, în principal, la drepturile acordate şi sînt îndrumaţi de către administratorii de securitate.

887. Utilizatorii trebuie să deţină autorizaţie de acces la secretul de stat de forma corespunzătoare gradului de secretizare a informaţiilor stocate, procesate sau transmise în SPAD sau RTD – SIC. La acordarea dreptului de acces la informaţii, se stabileşte, individual, necesitatea de a lucra cu informaţiile atribuite la secret de stat.

888. Informarea utilizatorilor cu îndatoririle lor de securitate trebuie să asigure o eficacitate sporită a sistemului de securitate.

889. Vizitatorii trebuie să aibă autorizaţie de acces de gradul corespunzător şi să îndeplinească principiul necesităţii de a lucra cu informaţii atribuite la secret de stat. În situaţia în care accesul unui vizitator fără drept de acces este considerat necesar, vor fi luate măsuri de securitate suplimentare pentru ca acesta să nu poată avea acces la informaţiile atribuite la secret de stat.

Secţiunea a 3-a

Condiţii de securitate

890. Utilizatorilor SPAD şi RTD – SIC li se acordă dreptul de acces la secretul de stat, în funcţie de necesitatea acestora de a lucra cu informaţii atribuite la secret de stat şi corespunzător gradului de secretizare a informaţiilor stocate, procesate sau transmise prin aceste sisteme

891. Autorităţile publice sau alte persoane juridice deţinătoare de informaţii atribuite la secret de stat în format electronic au obligaţia să instituie măsuri speciale pentru instruirea şi supravegherea personalului, inclusiv a personalului de proiectare de sistem care are acces la SPAD şi RTD, în vederea prevenirii şi înlăturării vulnerabilităţilor faţă de accesarea neautorizată.

892. În proiectarea SPAD şi RTD – SIC trebuie să se aibă în vedere ca atribuirea sarcinilor şi responsabilităţilor personalului să se facă în aşa fel încît

să nu existe o persoană care să aibă cunoştinţe sau acces la toate programele şi cheile de securitate – parole, mijloace de identificare personală.

893. Procedurile de lucru ale personalului din SPAD şi RTD – SIC trebuie să asigure separarea operaţiunilor de programare şi a celor de exploatare a sistemului sau reţelei. Nu se admite, cu excepţia unor situaţii speciale, ca personalul să facă atît programarea, cît şi operarea sistemelor sau reţelelor şi trebuie instituite proceduri speciale pentru depistarea acestor situaţii.

894. Pentru orice fel de modificare aplicată unui sistem SPAD sau RTD – SIC este obligatorie colaborarea a cel puţin două persoane – „regula celor doi". Procedurile de securitate trebuie să stabilească explicit situaţiile în care „regula celor doi" trebuie aplicată.

895. Pentru a asigura implementarea corectă a măsurilor de securitate, personalul SPAD şi RTD – SIC şi personalul care răspunde de securitatea acestora trebuie să fie instruit şi informat astfel încît să-şi cunoască reciproc atribuţiile.

896. Zonele în care sînt amplasate SPAD şi/sau RTD – SIC şi cele cu terminale la distanţă, în care sînt prezentate, stocate, procesate sau transmise informaţii atribuite la secret de stat ori în care este posibil accesul potenţial la astfel de informaţii, se declară zone de securitate clasa I sau clasa a II-a ale obiectivului şi se supun măsurilor de protecţie fizică stabilite de prezentul Regulament.

897. În zonele în care sînt amplasate sisteme SPAD şi terminale la distanţă – staţii de lucru, unde se procesează şi/sau pot fi accesate informaţii atribuite la secret de stat, se aplică următoarele măsuri generale de securitate:

1) intrarea personalului (introducerea materialelor), precum şi plecarea în/din aceste zone sînt controlate prin mijloace bine stabilite;

2) zonele şi locurile în care securitatea SPAD sau RTD – SIC sau a terminalelor la distanţă poate fi modificată nu trebuie să fie niciodată ocupate de o singură persoană autorizată;

3) persoanelor care solicită acces temporar sau cu intermitenţe în aceste zone trebuie să li se autorizeze accesul, ca vizitatori. Vizitatorii vor fi însoţiţi permanent, pentru a avea garanţia că nu pot avea acces la informaţiile atribuite la secret de stat şi nici la echipamentele utilizate.

898. În funcţie de riscul de securitate şi de gradul de secretizare a informaţiilor stocate, procesate şi transmise, se impune cerinţa de aplicare a regulii de lucru cu două persoane şi în alte zone, care vor fi stabilite în stadiul iniţial al proiectului şi prezentate în cadrul CSS.

899. Cînd un SPAD este exploatat în mod autonom, deconectat în mod permanent de alte SPAD, ţinînd cont de condiţiile specifice, de alte măsuri de securitate, tehnice sau procedurale şi de rolul pe care îl are respectivul SPAD

în funcţionarea de ansamblu a sistemului, organul competent pentru protecţia secretului de stat va stabili măsuri specifice de protecţie, adaptate la structura acestui SPAD, conform gradului de secretizare a informaţiilor gestionate.

900. Toate informaţiile şi materialele care privesc accesul la un SPAD sau RTD – SIC sînt controlate şi protejate prin reglementări corespunzătoare gradului cel mai înalt de secretizare şi specificului informaţiilor la care respectivul SPAD sau RTD – SIC permite accesul.

901. Cînd nu mai sînt utilizate, informaţiile şi materialele specificate în punctul 900 la prezentul Regulament trebuie să fie distruse, conform prevederilor prezentului Regulament.

902. Informaţiile atribuite la secret de stat în format electronic trebuie să fie controlate conform regulilor INFOSEC, înainte de a fi transmise din zonele SPAD şi RTD – SIC sau din cele cu terminale la distanţă.

903. Modul în care este prezentată informaţia în clar, chiar dacă se utilizează codul prescurtat de transmisie sau reprezentarea binară ori alte forme de transmitere la distanţă, nu trebuie să influenţeze gradul de secretizare acordat informaţiilor respective.

904. Cînd informaţiile sînt transferate între diverse SPAD sau RTD – SIC, ele trebuie să fie protejate atît în timpul transferului, cît şi la nivelul sistemelor informatice ale beneficiarului, corespunzător gradului de secretizare a informaţiilor transmise.

905. Toate mediile de stocare, purtătorii materiali ai informaţiilor se păstrează într-o modalitate care să corespundă celui mai înalt grad de secretizare a informaţiilor stocate.

906. Copierea informaţiilor atribuite la secret de stat, situate pe medii de stocare specifice TIC, se execută în conformitate cu prevederile din procedurile operaţionale de securitate.

907. Mediile reutilizabile de stocare a informaţiilor, folosite pentru înregistrarea informaţiilor atribuite la secret de stat, îşi menţin cel mai înalt grad de secretizare pentru care au fost utilizate anterior, pînă cînd respectivelor informaţii li se reduce gradul de secretizare sau sînt desecretizate, moment în care parafa de secretizare, aplicată mediilor sus-menţionate, se modifică în mod corespunzător sau aceste medii sînt distruse.

908. Evidenţa automată a accesului la informaţiile atribuite la secret de stat în format electronic se ţine în registrele de acces şi trebuie realizată necondiţionat prin software.

909. Registrele de acces se păstrează pe o perioadă stabilită de comun acord între organul competent pentru protecţia secretului de stat şi SSTIC.

910. Perioada minimă de păstrare a registrelor de acces la informaţiile

secretizate cu parafa „Strict secret” este de 10 ani, iar a registrelor de acces la informaţiile avînd gradele de secretizare „Secret”, „Confidenţial” şi „Restricţionat” – de cel puţin 3 ani.

911. Mediile de stocare care conţin informaţii atribuite la secret de stat, utilizate în interiorul unei zone SPAD, pot fi manipulate ca material unic secret, cu condiţia ca materialul să fie identificat, marcat cu parafa sa de secretizare şi controlat în interiorul zonei SPAD, pînă la momentul în care este distrus sau transmis pentru păstrare.

912. Evidenţele acestora vor fi menţinute în cadrul zonei SPAD pînă în momentul în care vor fi supuse controlului sau distruse.

913. În cazul în care un mediu de stocare este generat într-un SPAD sau RTD – SIC, iar apoi este transmis într-o zonă cu terminal/staţie de lucru la distanţă, se stabilesc proceduri adecvate de securitate, aprobate de către organul competent pentru protecţia secretului de stat. Procedurile trebuie să cuprindă şi instrucţiuni specifice privind evidenţa informaţiilor în format electronic.

914. Toate mediile de stocare secrete se verifică periodic, cel puţin anual, corespunzător gradului de secretizare.

915. Controlul periodic al mediilor de stocare se efectuează de către o comisie specială creată în modul stabilit de capitolul III, secţiunea a 11-a din prezentul Regulament, care trebuie să verifice prezenţa fizică a mediilor de stocare, precum şi conţinutul acestora în vederea corespunderii gradului de secretizare atribuit anterior.

916. Informaţiile atribuite la secret de stat, înregistrate pe medii de stocare reutilizabile, se şterg doar în conformitate cu procedurile operaţionale de securitate.

917. Cînd un mediu de stocare urmează să iasă din uz, trebuie să fie desecretizat, suprimîndu-se orice marcaje de secretizare, ulterior putînd fi utilizat ca mediu de stocare nesecret. Dacă acesta nu poate fi desecretizat, trebuie distrus în modul stabilit de prezentul Regulament.

918. Sînt interzise desecretizarea şi reutilizarea mediilor de stocare care conţin informaţii avînd gradul de secretizare „Strict secret”, acestea putînd fi numai distruse.

919. Informaţiile atribuite la secret de stat în format electronic, stocate pe un mediu de unică folosinţă – cartele, benzi perforate, trebuie distruse.

Secţiunea a 4-a

Reguli generale de securitate TIC

920. Toate mijloacele folosite pentru transmiterea electromagnetică a informaţiilor atribuite la secret de stat se supun instrucţiunilor de securitate a comu-

nicaţiilor, emise de către organul competent pentru protecţia secretului de stat.

921. Într-un SPAD - SIC trebuie să se dispună mijloace de interzicere a accesului la informaţiile atribuite la secret de stat de la toate terminalele/staţiile de lucru la distanţă, atunci cînd se solicită acest lucru, prin deconectare fizică sau prin proceduri software speciale, aprobate de organul competent pentru protecţia secretului de stat.

922. Instalarea iniţială a SPAD sau RTD – SIC sau orice modificare majoră adusă acestora vor fi executate de persoane autorizate, în condiţiile prezentului Regulament. Lucrările vor fi permanent supravegheate de personal tehnic calificat, care are drept de acces la secretul de stat de forma corespunzătoare celui mai înalt grad de secretizare a informaţiilor pe care respectivul SPAD sau RTD – SIC le va stoca, procesa sau transmite.

923. Toate echipamentele SPAD şi RTD-SIC vor fi instalate în conformitate cu reglementările specifice în vigoare, emise de către organul competent pentru protecţia secretului de stat şi standardele tehnice corespunzătoare.

924. Sistemele SPAD şi RTD-SIC, care stochează, procesează sau transmit informaţii secrete de stat, vor fi protejate corespunzător faţă de vulnerabilităţile de securitate cauzate de radiaţiile compromiţătoare – TEMPEST.

925. Procesarea informaţiilor se realizează în conformitate cu procedurile operaţionale de securitate, prevăzute de prezentul Regulament.

926. Transmiterea informaţiilor atribuite la secret de stat către instalaţii automate, a căror funcţionare nu necesită prezenţa unui operator uman, este interzisă, cu excepţia cazului în care se aplică reglementări speciale aprobate de organul competent pentru protecţia secretului de stat, iar acestea au fost specificate în procedurile operaţionale de securitate.

927. Procedurile operaţionale de securitate reprezintă descrierea implementării strategiei de securitate ce urmează să fie adoptată, a procedurilor operaţionale de urmat şi a responsabilităţilor personalului.

928. Procedurile operaţionale de securitate sînt elaborate de către SSTIC în colaborare cu organul competent pentru protecţia secretului de stat, precum şi cu alte autorităţi cu atribuţii în domeniu. Organul competent pentru protecţia secretului de stat va aproba procedurile de operare înainte de a autoriza stocarea, procesarea sau transmiterea informaţiilor secrete de stat prin SPAD – RTD – SIC.

929. SSTIC are obligaţia să efectueze controale periodice, prin care să stabilească dacă toate produsele software originale – sisteme de operare generale, subsisteme şi pachete soft, aflate în folosinţă, sînt protejate în condiţii corespunzătoare gradului de secretizare a informaţiilor pe care acestea trebuie să le proceseze. Protecţia aplicaţiilor software se stabileşte pe baza evaluării gradului de secretizare a acestora, ţinînd cont de gradul de secretizare a

informaţiilor pe care urmează să le proceseze.

930. Este interzisă utilizarea de software necertificate de către organul competent pentru protecţia secretului de stat.

931. Conservarea exemplarelor originale, a copiilor – backup sau off-site, precum şi salvările periodice ale datelor obţinute prin procesare vor fi executate în conformitate cu prevederile procedurilor operaţionale de securitate.

932. Versiunile software care sînt în uz trebuie să fie verificate la intervale regulate, pentru a garanta integritatea şi funcţionarea lor corectă.

933. Versiunile noi sau modificate ale software-ului nu vor fi folosite pentru procesarea informaţiilor atribuite la secret de stat, pînă cînd procedurile de securitate ale acestora nu sînt testate şi aprobate conform CSS.

934. Un software care îmbunătăţeşte posibilităţile sistemului şi care nu are nici o procedură de securitate nu poate fi folosit înainte de a fi verificat de către SSTIC.

935. Verificarea prezenţei viruşilor şi software-ului nociv se face în conformitate cu cerinţele stabilite de către organul competent pentru protecţia secretului de stat.

936. Versiunile de software noi sau modificate – sisteme de operare, subsisteme, pachete de software şi aplicaţii de software, stocate pe diferite medii, care se introduc într-o autoritate publică sau altă persoană juridică, trebuie verificate obligatoriu pe sisteme de calcul izolate, în vederea depistării software-ului nociv sau a viruşilor de calculator, înainte de a fi folosite în SPAD sau RTD – SIC. Periodic se va proceda la verificarea software-ului instalat.

937. Verificările trebuie făcute mai frecvent dacă SPAD sau RTD – SIC sînt conectate la alt SPAD sau RTD – SIC sau la o reţea publică de comunicaţii.

938. În contractele de întreţinere a SPAD şi RTD – SIC care stochează, procesează sau transmit informaţii atribuite la secret de stat se vor specifica cerinţele care trebuie îndeplinite pentru ca personalul de întreţinere şi aparatura specifică a acestuia să poată fi introduse în zona de operare a sistemelor respective.

939. Personalul de întreţinere trebuie să deţină autorizaţie de acces la secret de stat de forma corespunzătoare gradului de secretizare a informaţiilor la care au acces.

940. Scoaterea echipamentelor sau a componentelor hardware din zona SPAD sau RTD – SIC se execută în conformitate cu prevederile procedurilor operaţionale de securitate.

941. Cerinţele menţionate în punctul 938 şi punctul 939 din prezentul Regulament trebuie stipulate în CSS, iar procedurile de desfăşurare a activităţii

respective trebuie stabilite în procedurile operaţionale de securitate. Nu se acceptă tipurile de întreţinere care constau în aplicarea unor proceduri de diagnosticare ce implică accesul de la distanţă la sistem, decît în cazul în care activitatea respectivă se desfăşoară sub control strict şi numai cu aprobarea organului competent pentru protecţia secretului de stat.

942. Componentele sistemelor de securitate implementate în SPAD sau RTD – SIC trebuie certificate sau autorizate pe baza unei documentaţii tehnice amănunţite privind proiectarea, realizarea şi modul de distribuire al acestora.

943. SPAD sau RTD – SIC care stochează, procesează sau transmit informaţii atribuite la secret de stat sau componentele lor de bază – sisteme de operare de scop general, produse de limitare a funcţionării pentru realizarea securităţii şi produse pentru comunicare în reţea, se pot achiziţiona numai dacă au fost evaluate şi autorizate sau evaluate şi certificate de către organul competent pentru protecţia secretului de stat.

944. La închirierea unor componente hardware sau software, în special a unor medii de stocare, se va ţine cont că astfel de echipamente, odată utilizate în SPAD sau RTD - SIC ce procesează, stochează sau transmit informaţii atribuite la secret de stat, vor fi supuse măsurilor de protecţie reglementate prin prezentul Regulament. La secretizare, componentele respective nu vor putea fi scoase din zonele SPAD sau RTD – SIC decît după desecretizare.

945. Toate SPAD şi RTD – SIC, înainte de a fi utilizate pentru stocarea, procesarea sau transmiterea informaţiilor atribuite la secret de stat, trebuie certificate sau autorizate de către organul competent pentru protecţia secretului de stat, pe baza datelor stabilite în CSS, procedurilor operaţionale de securitate şi altor documentaţii relevante.

946. Subsistemele SPAD şi RTD – SIC şi staţiile de lucru cu acces la distanţă sau terminalele sînt certificate sau autorizate ca parte integrantă a sistemelor SPAD şi RTD – SIC la care sînt conectate.

947. În situaţiile referitoare la modul de operare de securitate multinivel, SPAD sau RTD – SIC, hardware-ul, firmware-ul şi software-ul, organul competent pentru protecţia secretului de stat stabileşte, în vederea evaluării şi certificării, criterii diferenţiate pentru fiecare grad de secretizare a informaţiilor vehiculate de SPAD sau RTD – SIC.

948. Cerinţele de evaluare şi certificare se includ în planificarea sistemului SPAD şi RTD – SIC şi sînt stipulate explicit în CSS, imediat după ce modul de operare de securitate a fost stabilit.

949. Evaluarea şi certificarea de securitate în modul de operare de securitate multinivel se impune:

1) pentru SPAD sau RTD – SIC care stochează, procesează sau transmite informaţii secretizate cu parafa „Strict secret”;

2) pentru SPAD sau RTD – SIC care stochează, procesează sau transmite informaţii secretizate cu parafa „Secret”, în cazurile în care:

a) SPAD sau RTD – SIC este interconectat cu un alt SPAD sau RTD – SIC, de exemplu, aparţinînd altui SSTIC;

b) SPAD sau RTD – SIC are un număr de utilizatori posibili care nu poate fi definit exact.

950. Procesele de evaluare şi certificare se efectuează de către experţi (specialişti cu pregătire tehnică adecvată), selecţionaţi de către organul competent pentru protecţia secretului de stat, care dispun de drept de acces la secret de stat de forma corespunzătoare.

951. În procesele de evaluare şi certificare se va stabili în ce măsură un SPAD sau RTD – SIC îndeplineşte condiţiile de securitate specificate prin CSS, avîndu-se în vedere că, după încheierea procesului de evaluare şi certificare, anumite secţiuni – paragrafe sau capitole, din CSS trebuie să fie modificate sau actualizate.

952. Procesele de evaluare şi certificare trebuie să înceapă din stadiul de definire a SPAD sau RTD – SIC şi să continue pe parcursul fazelor de dezvoltare.

953. Pentru toate SPAD şi RTD – SIC care stochează, procesează sau transmit informaţii atribuite la secret de stat, SSTIC stabileşte proceduri de control prin care să se poată stabili dacă schimbările intervenite în SIC sînt de natură a le compromite securitatea.

954. Modificările care implică o certificare repetată sau pentru care se solicită aprobarea anterioară a organului competent pentru protecţia secretului de stat trebuie să fie identificate cu claritate şi expuse în CSS.

955. După orice modificare, reparare sau eroare care ar fi putut afecta dispozitivele de securitate ale SPAD sau RTD – SIC, SSTIC trebuie să efectueze o verificare privind funcţionarea corectă a dispozitivelor de securitate.

956. Certificarea sau autorizarea SPAD sau RTD – SIC trebuie să corespundă nivelului de satisfacere a criteriilor de verificare.

957. Toate SPAD şi RTD – SIC care stochează, procesează sau transmit informaţii atribuite la secret de stat sînt inspectate şi reexaminate periodic de către organul competent pentru protecţia secretului de stat.

958. Pentru SPAD sau RTD – SIC care stochează, procesează sau transmit informaţii secretizate cu parafa „Strict secret”, inspecţia se va face cel puţin o dată pe an.

959. Microcalculatoarele sau calculatoarele personale care au discuri fixe sau alte medii nevolatile de stocare a informaţiei, ce operează autonom sau ca parte a unei reţele, precum şi calculatoarele portabile cu discuri fixe sînt considerate

medii de stocare a informaţiilor, în acelaşi sens ca şi celelalte medii amovibile de stocare a informaţiilor.

960. În măsura în care microcalculatoarele sau calculatoarele personale stochează informaţii atribuite la secret de stat, acestea trebuie supuse cerinţelor prezentului Regulament.

961. Echipamentelor prevăzute în punctul 959 din prezentul Regulament trebuie să li se acorde gradul de protecţie pentru acces, manipulare, stocare şi transport, corespunzător celui mai înalt grad de secretizare a informaţiilor care au fost vreodată stocate sau procesate pe ele, pînă la trecerea la un alt grad de secretizare sau desecretizarea lor, în conformitate cu procedurile legale.

962. Este interzisă utilizarea mediilor de stocare amovibile, a software-ului şi a hardware-ului, aflate în proprietate privată, pentru stocarea, procesarea şi transmiterea informaţiilor secrete de stat.

963. Este interzisă introducerea mediilor de stocare amovibile, a software-ului şi hardware-ului, aflate în proprietate privată, în zonele în care se stochează, se procesează sau se transmit informaţii atribuite la secret de stat, fără aprobarea conducătorului autorităţii publice sau al altei persoane juridice.

964. Utilizarea într-un obiectiv a echipamentelor şi a software-ului contractanţilor pentru stocarea, procesarea sau transmiterea informaţiilor atribuite la secret de stat este permisă numai cu avizul SSTIC şi aprobarea conducătorului autorităţii publice sau al altei persoane juridice.

965. Utilizarea într-un obiectiv a echipamentelor şi software-ului puse la dispoziţie de către alte instituţii poate fi permisă numai cu avizul SSTIC. În acest caz, echipamentele sînt evidenţiate în inventarul autorităţii publice sau al altei persoane juridice.

Capitolul XI

MĂSURI DE PROTECŢIE A SECRETULUI DE STAT LA EFECTUAREA UNOR LUCRĂRI COMUNE ŞI ALTOR LUCRĂRI

966. Autorităţile publice, alte persoane juridice, cetăţenii pot efectua lucrări comune sau alte lucrări cu utilizarea informaţiilor atribuite la secret de stat, în baza contractelor secretizate în modul stabilit de prezentul Regulament.

967. Pentru participarea la încheierea şi derularea contractelor cu utilizarea informaţiilor atribuite la secret de stat, persoanele juridice trebuie să dispună de certificat de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor avînd un anumit grad de secretizare, iar cetăţenii – să dispună de drept de acces la informaţiile atribuite la secret de stat de forma corespunzătoare.

968. Clauzele şi procedurile de protecţie a informaţiilor atribuite la secret de stat, devenite sau care pot deveni cunoscute în procesul încheierii şi derulării contractelor în legătură cu efectuarea unor lucrări comune sau altor lucrări, vor

fi stipulate în anexa de securitate a fiecărui contract, care presupune acces la astfel de informaţii.

969. Anexa de securitate se întocmeşte de beneficiar şi include toate măsurile, drepturile şi obligaţiile reciproce ale părţilor de asigurare a integrităţii şi protecţiei informaţiilor atribuite la secret de stat, atît în procesul derulării contractului, cît şi după încetarea acestuia.

970. Clauzele şi procedurile de protecţie vor fi supuse, periodic, inspecţiilor şi verificărilor de către organul competent pentru protecţia secretului de stat.

971. Beneficiarul este responsabil pentru secretizarea şi definirea tuturor componentelor acestuia, în conformitate cu normele în vigoare.

972. La secretizarea contractelor se vor aplica următoarele reguli generale:

1) în toate stadiile de planificare şi executare, gradul de secretizare a contractului se determină în funcţie de conţinutul informaţiilor utilizate;

2) secretizarea se aplică numai acelor părţi ale contractului care trebuie protejate;

3) dacă în derularea unui contract se folosesc informaţii din mai multe surse, cu grade de secretizare diferite, contractul va fi secretizat în funcţie de gradul cel mai înalt al informaţiilor, iar măsurile de protecţie vor fi stabilite în modul corespunzător;

4) desecretizarea sau modificarea gradului de secretizare a unei informaţii din cadrul contractului se aprobă de conducătorul autorităţii publice sau al altei persoane juridice care a aprobat secretizarea iniţială.

973. În cazul în care apare necesitatea protejării informaţiilor dintr-un contract care, anterior, nu a fost necesar a fi secretizat, beneficiarul are obligaţia declanşării procedurilor de secretizare şi protejare, conform reglementărilor în vigoare.

974. Contractantul poate ceda unui subcontractant realizarea unei părţi din contractul secretizat, doar cu acordul beneficiarului sau, dacă acest drept este prevăzut în contract, cu informarea obligatorie a beneficiarului. Subcontractantul trebuie să dispună de certificat de securitate.

975. Contractantul (executantul) şi subcontractanţii sînt obligaţi să implementeze şi să respecte toate măsurile de protecţie a informaţiilor atribuite la secret de stat puse la dispoziţie sau care au fost generate pe timpul derulării contractelor.

976. Transmiterea informaţiilor atribuite la secret de stat contractanţilor (executanţilor), în legătură cu efectuarea acestor lucrări, se face de către beneficiarul acestor lucrări, cu permisiunea autorităţii publice cu împuterniciri de dispoziţie asupra acestor informaţii şi numai în volumul necesar pentru

efectuarea lucrărilor respective.

977. Toate informaţiile atribuite la secret de stat, necesare derulării contractelor, se transmit prin intermediul Subdiviziunilor de protecţie, în modul stabilit de prezentul Regulament.

978. În timpul efectuării lucrărilor comune, a altor lucrări şi a apariţiei, în legătură cu aceasta, a necesităţii de a utiliza informaţii atribuite la secret de stat, persoanele juridice, inclusiv cele cu capital privat, pot încheia cu alte persoane juridice, care dispun de certificat de securitate, contracte de folosire a serviciilor prestate de către subdiviziunile lor de protecţie, fapt ce se notifică în certificatul de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor atribuite la secret de stat.

979. Dacă în timpul derulării contractului, executantul încalcă obligaţiile de protecţie a secretului de stat, beneficiarul are dreptul să suspende executarea comenzii pînă la lichidarea încălcărilor, iar în cazul încălcărilor repetate – să solicite anularea comenzii şi a certificatului de securitate pentru efectuarea lucrărilor cu utilizarea informaţiilor atribuite la secret de stat şi tragerea la răspundere a persoanelor vinovate.

980. Prejudiciul material cauzat de către executant statului, în persoana beneficiarului, se repară conform legislaţiei.

Capitolul XII

CONTROLUL PRIVIND STAREA PROTECŢIEI SECRETULUI DE STAT

Secţiunea 1

Dispoziţii generale

981. Controlul privind asigurarea protecţiei secretului de stat se efectuează de:

1) conducătorii autorităţilor publice şi ai altor persoane juridice, precum şi de Subdiviziunile de protecţie ale acestora;

2) Serviciul de Informaţii şi Securitate.

982. Conducătorii autorităţilor publice şi ai altor persoane juridice, Subdiviziunile de protecţie ale acestora exercită controlul privind asigurarea protecţiei secretului de stat referitor la informaţiile deţinute de acestea sau de persoanele juridice din subordine, precum şi cu privire la informaţiile transmise antreprenorilor în legătură cu executarea comenzilor.

983. Controlul privind asigurarea protecţiei secretului de stat în aparatele Parlamentului, Preşedintelui Republicii Moldova şi Guvernului este organizat

de către conducătorii acestor organe.

984. Serviciul de Informaţii şi Securitate este abilitat cu exercitarea controlului privind starea protecţiei secretului de stat în cadrul autorităţilor publice (control interdepartamental) şi în cadrul altor persoane juridice.

985. Controlul are ca scop:

1) evaluarea eficienţei măsurilor concrete de protecţie adoptate la nivelul deţinătorilor de informaţii atribuite la secret de stat, în conformitate cu Legea, cu prevederile prezentului Regulament şi ale altor norme în materie, precum şi cu programele de prevenire a scurgerii de informaţii atribuite la secret de stat;

2) identificarea neajunsurilor existente în sistemul de protecţie a informaţiilor atribuite la secret de stat, care ar putea conduce la divulgarea sau pierderea acestor informaţii, în vederea luării măsurilor de prevenire şi lichidare ce se impun;

3) constatarea cauzelor apariţiei acestor neajunsuri;

4) luarea măsurilor de remediere a deficienţelor şi elaborarea propunerilor de perfecţionare a cadrului organizatoric şi funcţional la nivelul autorităţii publice sau al altei persoane juridice controlate;

5) constatarea cazurilor de încălcare a normelor de protecţie a secretului de stat şi întreprinderea măsurilor necesare în vederea tragerii la răspundere a persoanelor vinovate de aceste încălcări.

986. Fiecare acţiune de control se încheie printr-un document de constatare, întocmit de persoana/persoanele care 1-au efectuat.

987. Concluziile formulate de către Serviciul de Informaţii şi Securitate în urma controlului sînt executorii pentru persoanele cu funcţii de răspundere ale autorităţilor publice sau ale altor persoane juridice controlate, acestea urmînd să adopte măsuri imediate de remediere a deficienţelor constatate.

988. În funcţie de obiectivele urmărite, controalele pot fi:

1) controale de fond (totale), care urmăresc verificarea întregului sistem organizatoric, structural şi funcţional de protecţie a informaţiilor atribuite la secret de stat;

2) controale tematice, care vizează anumite domenii ale activităţii de protecţie a informaţiilor atribuite la secret de stat;

3) controale în situaţii de urgenţă (operative), care au ca scop verificarea anumitor aspecte, stabilite ca urmare a identificării unui risc de securitate.

989. În funcţie de modul în care sînt stabilite şi organizate, controalele pot fi:

1) planificate;

2) inopinate.

990. Conducătorii autorităţilor publice sau ai altor persoane juridice care fac obiectul controlului au obligaţia să pună la dispoziţia reprezentanţilor Serviciului de Informaţii şi Securitate, care efectuează controlul, toate informaţiile solicitate privind modul de aplicare a măsurilor prevăzute de lege pentru protecţia secretului de stat.

991. Conducătorii autorităţilor publice sau ai altor persoane juridice deţinătoare de informaţii atribuite la secret de stat au obligaţia să organizeze, anual şi ori de cîte ori este nevoie, controale interne privind gestionarea acestora.

Secţiunea a 2-a

Investigaţii de serviciu

992. Faptele de divulgare a informaţiilor atribuite la secret de stat, pierdere a documentelor şi altor purtători materiali de informaţii atribute la secret de stat sau a articolelor care conţin asemenea informaţii se comunică neîntîrziat Subdiviziunii de protecţie, conducătorului autorităţii publice sau al altei persoane juridice (autorităţii cu împuterniciri de dispoziţie asupra acestor informaţii) şi Serviciului de Informaţii şi Securitate.

993. Totodată, în cazul încălcărilor menţionate în punctul 992 din prezentul Regulament se iau măsuri cu privire la organizarea unei investigaţii de serviciu pentru clarificarea circumstanţelor divulgării informaţiilor atribuite la secret de stat, pierderii documentelor, altor purtători materiali sau articolelor care conţin informaţii atribuite la secret de stat şi căutarea acestora. Măsurile necesare privind căutarea documentelor, altor purtători materiali de informaţii atribuite la secret de stat şi articolelor secrete, clarificarea circumstanţelor divulgării informaţiilor secrete şi depistarea persoanelor vinovate în cadrul autorităţilor publice sau altor persoane juridice se înfăptuiesc în comun cu Serviciul de Informaţii şi Securitate.

994. Pentru efectuarea investigaţiilor de serviciu, conducătorul autorităţii publice sau al altei persoane juridice, cel tîrziu a doua zi după descoperirea încălcării, instituie prin ordin o comisie formată din cel puţin 3 persoane competente şi imparţiale, inclusiv din cadrul Subdiviziunii de protecţie, care au acces de forma corespunzătoare gradului de secretizare a informaţiilor respective. În activitatea comisiei pot fi atraşi şi reprezentanţi ai autorităţilor publice sau altor persoane juridice ierarhic superioare.

995. Comisia care efectuează investigaţia de serviciu este obligată:

1) să stabilească circumstanţele divulgării informaţiilor atribuite la secret de stat, pierderii documentelor, altor purtători materiali sau articolelor care conţin asemenea informaţii (cum ar fi: timpul, locul, modul);

2) să caute documentul, alt purtător material de informaţii, articolul secret;

3) să stabilească persoanele care au comis încălcările respective;

4) să stabilească cauza şi condiţiile care au contribuit la divulgarea informaţiilor atribuite la secret de stat, pierderea, furtul documentelor, altor purtători materiali sau articolelor secrete şi să elaboreze recomandări pentru înlăturarea acestora.

996. Membrii comisiei care efectuează investigaţia de serviciu au dreptul:

1) să examineze încăperile autorităţii publice sau al altei persoane juridice, teritoriul adiacent, safeurile, dulapurile de metal, ambalajele, alţi suporţi speciali, mobilierul, valizele speciale, unde ar putea să se afle documentele, alţi purtători materiali de informaţii, articolele secrete pierdute;

2) să verifice, filă cu filă, documentaţia secretă şi registrele de evidenţă;

3) să chestioneze angajaţii autorităţii publice sau al altei persoane juridice care ar putea acorda un sprijin la elucidarea circumstanţelor cazului şi să obţină de la ei explicaţii (mărturii) în scris;

4) să atragă, cu permisiunea conducătorului autorităţii publice sau al altei persoane juridice respective, alţi angajaţi ai acesteia pentru organizarea unor măsuri de investigaţie aparte, cu asigurarea condiţiei de imparţialitate.

997. Investigaţia de serviciu trebuie să se efectueze în termen de cel mult o lună din ziua descoperirii faptului încălcării. În acest termen, conducătorul autorităţii publice sau al altei persoane juridice trebuie să soluţioneze, în modul stabilit, chestiunea privind tragerea la răspundere a persoanelor vinovate.

998. În cazul în care faptele săvîrşite constituie infracţiuni, autoritatea publică sau altă persoană juridică are obligaţia de a sesiza organele de urmărire penală şi de a pune la dispoziţia acestora datele şi materialele necesare probării acestora.

999. În cazul în care documentele, alţi purtători materiali sau articolele secrete pierdute nu au fost descoperite şi toate măsurile posibile de căutare s-au epuizat, au fost clarificate circumstanţele pierderii lor şi identificării persoanelor vinovate de aceasta, căutarea poate fi încetată. În legătură cu încetarea căutării se întocmeşte o concluzie motivată, care se aprobă de conducătorul autorităţii publice sau al altei persoane juridice şi, după caz, de către conducătorul autorităţii publice sau al altei persoane juridice ierarhic superioare.

1000. Rezultatele tuturor acţiunilor (măsurilor) întreprinse în procesul investigaţiei de serviciu se documentează.

1001. La finalizarea investigaţiei de serviciu, comisia este obligată să prezinte spre examinare conducătorului autorităţii publice sau al altei persoane juridice următoarele documente:

1) concluzia cu privire la rezultatele investigaţiei de serviciu;

2) explicaţiile scrise ale persoanelor chestionate de către membrii comisiei;

3) procesele-verbale privind verificarea documentelor, articolelor, încăperilor, safeurilor, altor suporţi speciali, mobilierului, valizelor speciale;

4) alte documente care se referă la investigaţia de serviciu.

1002. În procesul investigaţiei de serviciu comisia va determina inclusiv gradul de secretizare a informaţiilor divulgate, documentelor, altor purtători materiali de informaţii sau articolelor pierdute.

1003. Rezultatele activităţii cu privire la aprecierea gradului de secretizare a informaţiilor divulgate sau pierdute se reflectă, în termen de cel mult 10 zile de la data instituirii comisiei, într-o concluzie care se prezintă spre aprobare conducătorului autorităţii publice sau al altei persoane juridice.

1004. Dacă comisia stabileşte că gradul de secretizare a informaţiilor divulgate sau pierdute nu corespunde conţinutului acestora, atunci concluzia comisiei se aprobă de către conducătorul autorităţii publice sau al altei persoane juridice ierarhic superioare.

1005. Gradul se secretizare a informaţiilor divulgate sau pierdute, primite de la alte autorităţi publice sau persoane juridice se apreciază de către comisia formată din specialişti ai autorităţilor publice sau persoanelor juridice respective sau de către comisia instituţiei ierarhic superioare.

1006. Concluzia comisiei privind aprecierea gradului de secretizare a informaţiilor divulgate sau pierdute, cu anexarea, în caz de necesitate, a copiilor materialelor investigaţiei de serviciu se prezintă Subdiviziunii de protecţie, conducătorului autorităţii publice sau al altei persoane juridice, conducătorului autorităţii publice sau al altei persoane juridice ierarhic superioare, Serviciului de Informaţii şi Securitate.

1007. Un exemplar al concluziei şi materialele investigaţiei de serviciu se păstrează în Subdiviziunea de protecţie a autorităţii publice sau a altei persoane juridice.

1008. Subdiviziunea de protecţie are obligaţia de a ţine evidenţa cazurilor de încălcare a reglementărilor cu privire la secretul de stat, a documentelor de investigaţie şi a măsurilor luate în acest sens. Documentele menţionate se păstrează timp de cinci ani.

GUVERNUL

HOTĂRÎRE Nr. 411 din 25-05-2010

privind aprobarea Nomenclatorului informaţiilor atribuite la secret de stat

Publicat : 28-05-2010 în Monitorul Oficial Nr. 83-84 art. 483

Versiune în vigoare din 16.11.18 în baza modificărilor prin HG1106 din 14.11.18, MO424-429/16.11.18 art.1175

În temeiul art. 5 alin. (3) lit. c) şi art. 9 din Legea nr. 245-XVI din 27 noiembrie 2008 cu privire la secretul de stat (Monitorul Oficial al Republicii Moldova, 2009, nr. 45-46, art. 123), cu modificările ulterioare, Guvernul HOTĂRĂŞTE:

1. Se aprobă Nomenclatorul informaţiilor atribuite la secret de stat (se anexează).

2. Se stabileşte că autorităţile administraţiei publice centrale şi locale, alte persoane juridice de drept public şi privat, specificate în Nomenclatorul informaţiilor atribuite la secret de stat, sînt împuternicite să dispună, la cerere şi în limita competenţei lor, de informaţiile respective, precum şi de cele ale altor deţinători de informaţie.

3. În scopul concretizării şi sistematizării informaţiilor în domeniile lor de activitate, autorităţile administraţiei publice centrale şi locale, alte persoane juridice de drept public şi privat, specificate în Nomenclatorul informaţiilor atribuite la secret de stat, vor elabora, în baza şi în limitele acestuia, precum şi în conformitate cu art. 10 din Legea nr. 245-XVI din 27 noiembrie 2008 cu privire la secretul de stat, nomenclatoare departamentale detaliate de informaţii care urmează a fi secretizate.

Aprobat prin Hotărîrea Guvernului nr.411 din 25 mai 2010

NOMENCLATORUL

informaţiilor atribuite la secret de stat

Nr. crt.	Categoriile de informaţii atribuite la secret de stat	Autorităţile administraţiei publice centrale şi locale, alte persoane juridice de drept public şi privat, învestite să dispună, în limita competenţei, de informaţiile în cauză
1	2	3
	I. Informaţiile din domeniul apărării naţionale	
1.	Informaţiile ce dezvăluie conţinutul planurilor strategice şi operative, documentelor ce ţin de conducerea operaţiilor de luptă privind pregătirea şi derularea lor, desfăşurarea strategică, operativă şi de mobilizare a trupelor, conţinutul măsurilor ce ţin de acţiunile militare şi de asigurare a lor, de operaţiile internaţionale pe timp de pace şi de dirijare a luptei sau de trecerea de la timpul de pace la timpul de război a Forţelor Armate ale Republicii Moldova	Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Afacerilor Externe şi Integrării Europene, Serviciul de Informaţii şi Securitate, Serviciul de Protecţie şi Pază de Stat
2.	Informaţiile privind indicatorii importanţi ce caracterizează organizarea, efectivul, dislocarea, pregătirea de luptă şi de mobilizare, armamentul şi asigurarea tehnico-materială a Forţelor Armate ale Republicii Moldova	Ministerul Afacerilor Interne, Ministerul Apărării, Serviciul de Informaţii şi Securitate, Serviciul de Protecţie şi Pază de Stat
3.	Informaţiile ce dezvăluie conţinutul planurilor de aplicare a trupelor pe timp de pace în operaţii speciale (antiteroriste) şi în cadrul măsurilor de apărare a statului, societăţii şi persoanei contra acţiunilor anticonstituţionale şi violenţei armate ilegale	Ministerul Afacerilor Interne, Ministerul Apărării, Centrul Naţional Anticorupţie, Serviciul de Protecţie şi Pază de Stat, Ministerul Afacerilor Externe şi Integrării Europene

4.	Informaţiile ce dezvăluie conţinutul planurilor şi al măsurilor de pregătire operativă şi de luptă, planurilor de mobilizare (planurilor de demobilizare), documentelor privind dirijarea desfăşurării trupelor, pregătirea de mobilizare a trupelor, posibilităţile de completare a lor cu efectivul necesar, de asigurare cu armament, tehnică militară, mijloace de transport militare şi alte mijloace materiale şi financiare	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Afacerilor Interne, Ministerul Economiei, Ministerul Finanţelor, Serviciul de Protecţie şi Pază de Stat
5.	Informaţiile ce dezvăluie conţinutul planurilor de construcţie (perfecţionare) şi dezvoltare a trupelor, starea de pregătire de luptă şi de asigurare de luptă a acestora, efectivul forţelor (mijloacelor) de serviciu şi starea lor de pregătire de luptă, precum şi informaţiile ce conţin analiza situaţiei politico-militare şi operative	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Afacerilor Interne, Serviciul de Protecţie şi Pază de Stat
6.	Informaţiile ce dezvăluie direcţiile de dezvoltare a unor tipuri de armament, de tehnică militară şi specială, cantitatea şi caracteristicile lor tehnico-tactice, organizarea şi tehnologiile de producţie, lucrările ştiinţifice teoretice şi experimentale legate de crearea modelelor noi de armament, tehnică militară şi specială sau modernizarea acestora, alte lucrări planificate sau efectuate în interesele apărării naţionale	Serviciul de Informaţii şi Securitate, Academia de Ştiinţe a Moldovei, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Economiei, Serviciul de Protecţie şi Pază de Stat, Ministerul Afacerilor Externe şi Integrării Europene
7.	Informaţiile ce dezvăluie însuşirile, compoziţia şi tehnologia producerii substanţelor explozive, aliajelor noi, lichidelor speciale şi carburanţilor noi pentru armament şi tehnica militară, precum şi caracteristicile şi tehnologia producerii mijloacelor explozive cu destinaţie militară	Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Economiei, Academia de Ştiinţe a Moldovei, Serviciul de Protecţie şi Pază de Stat

8.	Informaţiile privind forţele şi mijloacele protecţiei civile, capacităţile de care dispun localităţile şi unele obiective separate pentru protecţia, evacuarea şi dispersarea populaţiei, asigurarea activităţilor sociale vitale ale populaţiei şi activităţii de producţie a persoanelor juridice în perioada de război, de asediu sau de urgenţă, precum şi în cazul situaţiilor excepţionale	Centrul Naţional Anticorupţie, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Economiei, Serviciul de Protecţie şi Pază de Stat, alte autorităţi administrative centrale, care în virtutea exercitării atribuţiilor lor, vor avea necesitatea de a dispune de astfel de informaţii
9.	Informaţiile ce dezvăluie dislocarea, destinaţia, gradul de pregătire şi de securitate a obiectivelor cu regim special şi punctelor de comandă de rezervă ale organelor centrale de specialitate ale administraţiei publice, proiectarea, construcţia şi exploatarea acestora, repartizarea terenului, subsolului şi acvatoriului pentru asemenea obiective	Centrul Naţional Anticorupţie, Ministerul Afacerilor Interne, Ministerul Apărării, Serviciul de Protecţie şi Pază de Stat, alte autorităţi administrative centrale, care, în virtutea exercitării atribuţiilor lor, vor avea necesitatea de a dispune de astfel de informaţii
10.	Informaţiile privind dislocarea, destinaţia, gradul de pregătire, denumirile autentice, structura organizatorică, dotarea cu armament, efectivul trupelor care, conform obligaţiilor internaţionale ale Republicii Moldova, nu pot fi accesibile publicului	Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Justiţiei, Serviciul de Protecţie şi Pază de Stat, Serviciul de Stat de Curieri Speciali
11.	Informaţiile ce dezvăluie organizarea şi funcţionarea tuturor tipurilor de comunicaţii necesare asigurării capacităţii de apărare şi securităţii statului, asigurării radiotehnice şi de radiolocaţie a trupelor, precum şi repartizarea şi utilizarea canalelor de radiofrecvenţe cu destinaţie militară sau specială	Centrul Naţional Anticorupţie, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Ministerul Afacerilor Externe şi Integrării Europene, Serviciul de Protecţie şi Pază de Stat

12.	Informaţiile geospaţiale privind teritoriul Republicii Moldova şi alte regiuni ale Pământului ce dezvăluie rezultatele activităţii topografice, geodezice şi cartografice de importanţă majoră pentru apărare sau economie	Agenţia Relaţii Funciare şi Cadastru, Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Afacerilor Interne, Ministerul Economiei, Serviciul de Protecţie şi Pază de Stat
13.	Informaţia cadastrală despre obiectivele şi comunicaţiile speciale	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Afacerilor Interne, Agenţia Relaţii Funciare şi Cadastru
14.	Informaţiile ce dezvăluie datele şi caracteristicile geodezice, gravimetrice, cartografice şi hidrometeorologice care prezintă importanţă pentru apărarea statului	Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Mediului, Agenţia Relaţii Funciare şi Cadastru
15.	Informaţiile privind utilizarea infrastructurii Republicii Moldova în scopul asigurării capacităţii de apărare şi securităţii statului, informaţiile privind indicii ce determină pregătirea economiei Republicii Moldova pentru o funcţionare stabilă pe timp de război şi pe timp de pace, inclusiv informaţiile ce dezvăluie structura organizatorică sau indicii planului de mobilizare a economiei Republicii Moldova	Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Serviciul de Protecţie şi Pază de Stat, Ministerul Economiei, Ministerul Finanţelor, Ministerul Apărării, Agenţia Rezerve Materiale, alte autorităţi administrative centrale, care, în virtutea exercitării atribuţiilor lor, vor avea necesitatea de a dispune de astfel de informaţii

16.	Informaţiile privind pregătirea de mobilizare şi mobilizarea organelor centrale de specialitate ale administraţiei publice şi a altor instituţii, precum şi informaţiile ce dezvăluie conţinutul planurilor, conţinutul sau rezultatele lucrărilor de cercetare ştiinţifică, experimentale de construcţii în domeniul pregătirii de mobilizare şi al mobilizării organelor centrale de specialitate ale administraţiei publice şi a altor instituţii, inclusiv pregătirea de mobilizare a economiei Republicii Moldova	Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Ministerul Apărării, Academia de Ştiinţe a Moldovei, Serviciul de Protecţie şi Pază de Stat, Ministerul Finanţelor, Ministerul Economiei, Ministerul Agriculturii şi Industriei Alimentare, alte autorităţi administrative centrale, care, în virtutea exercitării atribuţiilor lor, vor avea necesitatea de a dispune de astfel de informaţii
17.	Informaţiile privind rezervele şi volumul livrărilor de materiale strategice, datele generalizate despre nomenclatura şi nivelul stocurilor, volumul livrărilor, alocării, depunerii, împrospătării acestora, amplasarea şi volumul real al rezervelor materiale de stat şi de mobilizare, datele privind finanţarea lor	Serviciul de Informaţii şi Securitate, Ministerul Finanţelor, Ministerul Sănătăţii, Ministerul Transporturilor şi Infrastructurii Drumurilor, Ministerul Economiei, Ministerul Agriculturii şi Industriei Alimentare, Ministerul Mediului, Agenţia Rezerve Materiale

18.	Informaţiile ce dezvăluie posibilităţile de pregătire a drumurilor, căilor ferate, căilor navigabile interne, transportului naval şi aerian al Republicii Moldova pentru mobilizare în scopul asigurării securităţii statului şi siguranţei la transportarea încărcăturilor, precum şi al utilizării sau pregătirii pentru scopuri militare a reţelei de transport şi a mijloacelor de transport. Informaţiile ce dezvăluie volumele încărcăturilor speciale şi militare, organizarea transportării armamentului, tehnicii militare şi producţiei de alt gen, utilizate pentru necesităţi de apărare, precum şi rutele de transportare a acestora	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Afacerilor Interne, Ministerul Transporturilor şi Infrastructurii Drumurilor, Ministerul Economiei, Administraţia de Stat a Aviaţiei Civile, Ministerul Dezvoltării Regionale şi Construcţiilor, autorităţile administraţiei publice locale
19.	Informaţiile ce dezvăluie indicii comenzii de stat pentru apărarea naţională şi asigurarea securităţii statului, partea privind armamentul, tehnica militară şi specială, producţia cu destinaţie de apărare, precum şi capacităţile de producere a acestora Informaţiile privind cooperarea întreprinderilor, constructorii şi producătorii de armament, tehnică militară şi alte tipuri de producţie utilizată pentru necesităţile de apărare, dacă aceste informaţii dezvăluie datele despre capacităţile de producţie şi (sau) caracteristicile tehnico-tactice de bază ale armamentului şi tehnicii militare	Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Economiei
20.	Informaţiile privind capacitatea de mobilizare a unităţilor de producţie pentru fabricarea produselor de utilitate generală, incluse în sarcinile de mobilizare, privind tipurile de materie primă şi de materiale strategice, fabricarea şi reparaţia armamentului, tehnicii militare şi informaţiile privind crearea, dezvoltarea sau păstrarea acestor capacităţi	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Economiei
21.	Informaţiile ce caracterizează starea fondului de asigurare a documentaţiei pentru armament şi tehnica militară, tipurile principale de produse de utilitate generală, incluse în sarcinile de mobilizare, obiectele cu risc sporit sau sistemele de importanţă vitală pentru populaţie, obiectele ce constituie patrimoniu naţional Informaţiile privind dislocarea obiectelor (bazelor) de păstrare a fondului de asigurare a documentaţiei	Ministerul Apărării, Ministerul Afacerilor Interne, Ministerul Economiei, Serviciul de Informaţii şi Securitate

22.	Informaţiile privind planurile, volumul şi alte caracteristici importante referitoare la prospectarea şi exploatarea zăcămintelor minerale utile pe teritoriul Republicii Moldova, precum şi rezultatele lucrărilor în domeniul heliogeofizicii sau ale cercetărilor geologice şi geofizice speciale, efectuate în vederea asigurării capacităţii de apărare şi securităţii statului	Ministerul Mediului, Serviciul de Informaţii şi Securitate, Academia de Ştiinţe a Moldovei, Ministerul Economiei
23.	Informaţiile privind realizările ştiinţei şi tehnicii, mijloacele de asigurare metrologică ce determină nivelul calitativ nou al posibilităţilor armamentului şi tehnicii militare, ridicarea capacităţii lor de luptă	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Economiei, Academia de Ştiinţe a Moldovei
24.	Informaţiile ce dezvăluie conţinutul lucrărilor efectuate în scopul creării mijloacelor de detecţie, degazare, protecţie chimică, radiologică sau biologică contra armelor de distrugere în masă, a noilor materiale de absorbţie sau a materialelor de alt tip	Serviciul de Informaţii şi Securitate, Ministerul Economiei, Ministerul Apărării, Ministerul Afacerilor Interne, Ministerul Mediului
25.	Informaţiile ce dezvăluie direcţiile de dezvoltare a mijloacelor şi tehnologiilor cu destinaţie dublă, conţinutul şi rezultatele îndeplinirii programelor cu destinaţie specială, lucrărilor de cercetare ştiinţifică şi experimentale de construcţii, efectuate în vederea creării şi modernizării acestor mijloace şi tehnologii Informaţiile privind aplicarea mijloacelor şi tehnologiilor cu destinaţie dublă în scopuri militare	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Economiei, Academia de Ştiinţe a Moldovei, Ministerul Afacerilor Interne
26.	Informaţiile ce dezvăluie pronosticurile privind progresul tehnico-ştiinţific în Republica Moldova şi impactul social-economic pentru capacitatea de apărare şi securitatea statului	Serviciul de Informaţii şi Securitate, Academia de Ştiinţe a Moldovei, Ministerul Apărării, Ministerul Afacerilor Externe şi Integrării Europene, Ministerul Economiei
27.	Informaţiile cu privire la transportarea, circulaţia şi depozitarea metalelor şi pietrelor preţioase aflate în gestiunea autorităţilor centrale	Ministerul Finanţelor,Ministerul Afacerilor Interne, Serviciul de Informaţii şi Securitate, Banca Naţională a Moldovei.
28.	Informaţiile privind protecţia sistemelor informatice ale Băncii Naţionale a Moldovei a căror divulgare poate prejudicia sistemul bancar al Republicii Moldova	Banca Naţională a Moldovei, Serviciul de Informaţii şi Securitate

29.	Informaţiile privind proiectele de monede în curs de elaborare, cu excepţia celor jubiliare şi comemorative, şi de bancnote de model nou, pînă la publicarea lor oficială şi punerea lor în circulaţie	Banca Naţională a Moldovei, Ministerul Finanţelor, Serviciul de Informaţii şi Securitate
30.	Informaţiile despre metodele de protecţie contra falsificării bancnotelor sau a altor articole fabricate la comanda Băncii Naţionale a Moldovei	Ministerul Afacerilor Interne, Banca Naţională a Moldovei, Serviciul de Informaţii şi Securitate
31.	Informaţiile privind baterea monedelor şi tipărirea bancnotelor aflate în circulaţie, precum şi informaţiile cu privire la transportarea acestora, inclusiv a monedelor jubiliare şi acelor comemorative, de la producător la sediul Băncii Naţionale a Moldovei	Ministerul Afacerilor Interne, Banca Naţională a Moldovei, Ministerul Finanţelor, Serviciul de Informaţii şi Securitate
32.	Informaţiile despre problemele privind politica externă, comerţul exterior, relaţiile tehnico-ştiinţifice, care dezvăluie strategia şi tactica politicii externe a Republicii Moldova, a căror răspîndire prematură poate aduce prejudicii securităţii statului	Ministerul Afacerilor Externe şi Integrării Europene, Ministerul Economiei, Ministerul Finanţelor (Serviciul Vamal), Serviciul de Informaţii şi Securitate
33.	Informaţiile privind sursele informaţiilor confidenţiale în problemele politice, militare, tehnico-ştiinţifice şi economice referitoare la unul sau la mai multe state	Ministerul Afacerilor Externe şi Integrării Europene, Ministerul Economiei, Serviciul de Informaţii şi Securitate
34.	Informaţiile despre tratativele dintre reprezentanţii Republicii Moldova şi reprezentanţii altor state privind elaborarea unei poziţii unice în relaţiile internaţionale, dacă divulgarea acestor informaţii poate aduce prejudicii securităţii Republicii Moldova şi altor state	Ministerul Afacerilor Externe şi Integrării Europene, Ministerul Justiţiei, Serviciul de Informaţii şi Securitate
35.	Informaţiile privind pregătirea, încheierea şi ratificarea tratatelor internaţionale a căror divulgare prematură poate aduce prejudicii securităţii statului	Ministerul Afacerilor Externe şi Integrării Europene, Ministerul Justiţiei, Serviciul de Informaţii şi Securitate, Ministerul Finanţelor, Ministerul Economiei

36.	Informaţiile privind exportul şi importul de armament şi tehnică militară, reparaţia şi exploatarea acestora, privind acordarea asistenţei tehnice statelor străine în crearea de armament, tehnică militară, obiecte militare şi obiecte ce ţin de industria de apărare, privind acordarea de către Republica Moldova a asistenţei tehnico-militare statelor străine, dacă divulgarea acestor informaţii poate aduce prejudicii securităţii statului	Ministerul Apărării, Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Externe şi Integrării Europene, Ministerul Economiei
37.	Informaţiile ce dezvăluie, în ansamblu, balanţa de plăţi a Republicii Moldova cu statele străine pe timp de război	Ministerul Apărării, Ministerul Economiei, Banca Naţională a Moldovei, Serviciul de Informaţii şi Securitate, Ministerul Finanţelor, Ministerul Afacerilor Externe şi Integrării Europene
38.	Informaţiile ce dezvăluie forţele, mijloacele, sursele, metodele, planurile, rezultatele activităţii de recunoaştere şi de contrainformaţii, operative de investigaţii şi ale operaţiilor speciale (antiteroriste), precum şi datele privind finanţarea acestei activităţi şi a operaţiilor speciale, dacă datele respective dezvăluie informaţiile enumerate	Organele care desfăşoară activitate operativă de investigaţii, Ministerul Apărării, Ministerul Finanţelor, Procuratura Generală
38[1]	Informaţiile ce dezvăluie efectivul, forţele, conţinutul, planurile, organizarea, finanţarea şi asigurarea tehnico-materială, formele, tactica, metodele, mijloacele activităţilor de desfăşurare a testării integrităţii profesionale	Serviciul de Informaţii şi Securitate, Centrul Naţional Anticorupţie
39.	Informaţiile despre persoanele care acordă sau au acordat pe bază confidenţială sprijin organelor care desfăşoară activitate operativă de investigaţii în procesul desfăşurării activităţii operative	Organele care desfăşoară activitate operativă de investigaţii, Ministerul Apărării, Procuratura Generală

40.	Informaţiile privind pregătirea şi repartizarea personalului antrenat în acţiunile de asigurare a securităţii statului, colaboratorii organelor care desfăşoară activitate operativă de investigaţii, care îndeplinesc sau au îndeplinit misiuni speciale în serviciile speciale (organizaţiile) ale statelor străine, în cadrul grupărilor criminale străine sau locale, precum şi informaţiile privind asigurarea financiară a acestor activităţi	Serviciul de Informaţii şi Securitate, Procuratura Generală, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Justiţiei, Ministerul Finanţelor (Serviciul Vamal), Centrul Naţional Anticorupţie, Serviciul de Protecţie şi Pază de Stat
41.	Informaţiile ce dezvăluie măsurile tehnico-operative şi operative de căutare efectuate de subdiviziunile operative speciale	Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Justiţiei, Ministerul Finanţelor (Serviciul Vamal), Serviciul de Informaţii şi Securitate, Serviciul de Protecţie şi Pază de Stat, Centrul Naţional Anticorupţie, Procuratura Generală
42.	Informaţiile ce dezvăluie forţele, mijloacele şi metodele de efectuare a urmăririi penale în cauzele penale privind infracţiunile contra păcii şi securităţii omenirii, contra autorităţilor publice şi a securităţii statului, precum şi în cauzele penale în cadrul cărora, la etapa urmăririi penale, sînt examinate circumstanţele ce conţin informaţii atribuite la secret de stat	Organele de urmărire penală, Procuratura Generală, Serviciul de Informaţii şi Securitate
43.	Informaţiile ce dezvăluie forţele, mijloacele, metodele, planurile, mersul şi rezultatele activităţii subdiviziunilor de cercetare cu mijloace radioelectronice, precum şi datele privind finanţarea acestei activităţi, dacă datele respective dezvăluie informaţiile enumerate	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Afacerilor Interne, Ministerul Finanţelor, Ministerul Justiţiei
44.	Informaţiile ce dezvăluie planurile, organizarea, finanţarea, forţele, mijloacele şi metodele de asigurare a securităţii persoanelor beneficiare de protecţie de stat şi obiectelor care beneficiază de protecţie şi pază de stat	Serviciul de Informaţii şi Securitate, Serviciul de Protecţie şi Pază de Stat, Ministerul Afacerilor Interne, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Ministerul Justiţiei

45.	Informaţiile ce dezvăluie mijloacele şi metodele de protecţie a informaţiei care conţine date atribuite la secret de stat, măsurile planificate şi (sau) întreprinse în vederea protejării informaţiei contra accesului neautorizat al serviciilor tehnice de informaţii străine şi scurgerii prin canalele tehnice, precum şi datele privind finanţarea acestor măsuri, dacă datele respective dezvăluie informaţiile enumerate	Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Ministerul Apărării, alte instituţii care efectuează lucrări cu tematică închisă
46.	Informaţiile ce dezvăluie mijloacele, metodele, măsurile organizatorice, tehnice şi alte măsuri orientate spre asigurarea regimului secret	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Afacerilor Interne, Ministerul Finanţelor (Serviciul Vamal), Ministerul Justiţiei, Centrul pentru Centrul Naţional Anticorupţie
47.	Informaţiile ce dezvăluie forţele, mijloacele şi metodele de asigurare a protecţiei de stat părţii vătămate, martorilor şi altor persoane care acordă ajutor în procesul penal, precum şi datele privind finanţarea acestei activităţi, dacă datele respective dezvăluie informaţiile enumerate	Organele care acordă, conform competenţei, protecţie de stat martorilor şi altor participanţi la procesul penal, Serviciul de Informaţii şi Securitate
	Informaţiile ce dezvăluie forţele, mijloacele şi metodele de supraveghere a frontierei de stat a Republicii Moldova	Ministerul Afacerilor Interne, Serviciul de Informaţii şi Securitate
49.	Informaţiile privind sistemele guvernamentale de telecomunicaţii, sistemele de legătură guvernamentală cifrată, codificată şi secretizată, privind cifrurile, elaborarea şi fabricarea cifrurilor şi asigurarea cu cifruri, privind metodele sau procedurile de analiză a mijloacelor de cifrare şi a mijloacelor de protecţie specială, privind sistemele informaţional-analitice cu destinaţie specială	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Ministerul Afacerilor Interne, Serviciul de Protecţie şi Pază de Stat, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Cancelaria de Stat.

50.	Informaţiile privind utilizarea, protecţia şi dezvoltarea legăturilor interdependente în reţelele de comunicaţii ale Republicii Moldova, care funcţionează în scopul asigurării capacităţii de apărare şi securităţii statului	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Serviciul de Protecţie şi Pază de Stat, Ministerul Afacerilor Interne, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Ministerul Finanţelor (Serviciul Vamal), Ministerul Justiţiei, Cancelaria de Stat.
51.	Informaţiile privind mijloacele, circuitele, canalele şi sistemele de comunicaţii proprii şi închiriate ale organelor securităţii de stat	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Serviciul de Protecţie şi Pază de Stat, Ministerul Afacerilor Interne, Societatea pe Acţiuni „Moldtelecom” , Cancelaria de Stat.
52.	Informaţiile ce dezvăluie schemele generale şi schemele de dezvoltare a reţelelor magistrale de cabluri de importanţă statală şi a liniilor de transmisiuni prin radiorelee, prin satelit şi staţii radio, cu indicarea capacităţilor acestora şi a locului de amplasare (coordonatele geografice) în ansamblu pe republică	Serviciul de Informaţii şi Securitate, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Ministerul Apărării, Societatea pe Acţiuni „Moldtelecom” , Cancelaria de Stat.
53.	Informaţiile generalizate (cu schemele şi descrierea lor, care conţin coordonate geografice) despre nodurile de telecomunicaţii active şi de rezervă (reţelele de staţii radio, de transmisiuni prin radiorelee şi prin satelit, amplasate în nodurile de telecomunicaţii de rezervă), despre inelele de cablu şi radioreleele din cadrul organelor securităţii statului	Serviciul de Informaţii şi Securitate, Ministerul Apărării, Serviciul de Protecţie şi Pază de Stat, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Societatea pe Acţiuni „Moldtelecom” , Cancelaria de Stat.
54.	Informaţiile generalizate despre schemele canalelor pentru cabluri din centrele administrative ale Republicii Moldova	Serviciul de Informaţii şi Securitate, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Societatea pe Acţiuni „Moldtelecom” , Cancelaria de Stat.

55.	Informaţiile ce dezvăluie sistemele, mijloacele şi metodele de protejare a datelor importante pentru stat, care circulă, se păstrează şi se prelucrează în formă electronică	Serviciul de Informaţii şi Securitate, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Finanţelor (Serviciul Vamal), Centrul Naţional Anticorupţie, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Ministerul Justiţiei, Cancelaria de Stat.
56.	Informaţiile privind organizarea, conţinutul, starea şi planurile de dezvoltare a protecţiei criptografice şi tehnice a secretului de stat, conţinutul şi rezultatele cercetărilor ştiinţifice în domeniul criptografiei referitor la protecţia secretului de stat	Serviciul de Informaţii şi Securitate, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Academia de Ştiinţe a Moldovei, Cancelaria de Stat.
57.	Informaţiile privind sistemele, mijloacele de protecţie criptografică a secretului de stat, elaborarea cifrurilor de stat, proiectarea, producerea, tehnologiile de producere a acestora	Serviciul de Informaţii şi Securitate, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Cancelaria de Stat.
58.	Informaţiile privind utilizarea sistemelor, mijloacelor de protecţie criptografică a secretului de stat şi cifrurilor de stat	Serviciul de Informaţii şi Securitate, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Afacerilor Externe şi Integrării Europene, Serviciul de Protecţie şi Pază de Stat, Centrul Naţional Anticorupţie, Cancelaria de Stat.

59.	Informaţiile privind conţinutul extraselor, comentariilor, proiectelor, părţilor acestora, altor acte de uz intern ale autorităţilor publice, a căror divulgare ar putea conduce la divulgarea informaţiilor atribuite la secret de stat	Autorităţile administraţiei publice centrale şi locale, alte persoane juridice de drept public şi privat învestite să dispună de informaţiile atribuite la secret de stat, în conformitate cu punctele 1-58 din prezentul Nomenclator
60.	Informaţiile privind activitatea de elaborare, modificare, completare, definitivare a actelor oficiale, alte proceduri şi activităţi ale autorităţilor publice de colectare şi prelucrare a informaţiilor care, în modul prevăzut de legislaţie, urmează să fie atribuite la secret de stat	Autorităţile administraţiei publice centrale şi locale, alte persoane juridice de drept public şi privat învestite să dispună de informaţiile atribuite la secret de stat, în conformitate cu punctele 1-58 din prezentul Nomenclator
61.	Informaţiile privind activitatea de examinare şi deliberare în cadrul autorităţilor publice şi între acestea în problemele din domeniile în care informaţiile sînt atribuite la secret de stat	Autorităţile administraţiei publice centrale şi locale, alte persoane juridice de drept public şi privat învestite să dispună de informaţiile atribuite la secret de stat, în conformitate cu punctele 1-58 din prezentul Nomenclator

GUVERNUL

HOTĂRÎRE *Nr. 449 din 16-06-2011*

cu privire la aprobarea Nomenclatorului persoanelor cu funcţii de răspundere cu împuterniciri de atribuire a informaţiilor la secret de stat

Publicat : 24-06-2011 în Monitorul Oficial Nr. 103-106 art. 513

În temeiul articolului 5 alineatul (3) litera c) din Legea nr.245-XVI din 27 noiembrie 2008 cu privire la secretul de stat (Monitorul Oficial al Republicii Moldova, 2009, nr.45-46, art.123), cu modificările şi completările ulterioare, Guvernul HOTĂRĂŞTE:

Se aprobă Nomenclatorul persoanelor cu funcţii de răspundere cu împuterniciri de atribuire a informaţiilor la secret de stat (se anexează).

Anexă

la Hotărîrea Guvernului nr. 449 din 16-06-2011

NOMENCLATORUL

persoanelor cu funcţii de răspundere cu împuternici de atribuire a informaţiilor la secret de stat

Preşedintele Republicii Moldova

Preşedintele Parlamentului

Prim-ministrul

Membrii Guvernului

Secretarul general al Guvernului

Preşedintele Curţii Constituţionale

Preşedintele Curţii Supreme de Justiţie

Preşedintele Curţii de Conturi

Procurorul General

Guvernatorul Băncii Naţionale a Moldovei

Directorul Serviciului de Informaţii şi Securitate

Directorul Serviciului de Protecţie şi Pază de Stat

Directorul Serviciului de Stat de Curieri Speciali

Directorul general al Administraţiei de Stat a Aviaţiei Civile

Directorul general al S.A. „Moldtelecom”

Preşedintele Comisiei Naţionale a Pieţei Financiare

Conducătorii altor autorităţi administrative centrale prevăzute în art.24 al Legii nr. 64-XII din 31 mai 1990 cu privire la Guvern

Conducătorii autorităţilor publice centrale şi locale, alte persoane juridice de drept public şi privat învestite să dispună de informaţiile atribuite la secret de stat, în conformitate cu prevederile Nomenclatorului informaţiilor atribuite la secret de stat, aprobat prin Hotărîrea Guvernului nr.411 din 25 mai 2010

PARLAMENTUL

LEGEA Nr. 59 din 29-03-2012

privind activitatea specială de investigaţii

Publicat : 08-06-2012 în Monitorul Oficial Nr. 113-118 art. 373

Versiune în vigoare din *12.01.19 în baza modificărilor prin LP245 din 15.11.18* MO *462-466 din 12.12.18 art. 774*

Capitolul I
DISPOZIŢII GENERALE

Articolul 1. Noţiunea şi domeniul de reglementare a activităţii speciale de investigaţii

(1) Activitatea specială de investigaţii reprezintă o procedură cu caracter secret şi/sau public, efectuată de autorităţile competente, cu sau fără utilizarea echipamentelor tehnice speciale, în scopul culegerii de informaţii necesare pentru prevenirea şi combaterea criminalităţii, asigurarea securităţii statului, ordinii publice, apărarea drepturilor şi intereselor legitime ale persoanelor, descoperirea şi cercetarea infracţiunilor.

(2) Prezenta lege reglementează măsurile speciale de investigaţii, modalitatea de dispunere şi de efectuare a acestora, precum şi efectuarea controlului asupra legalităţii lor.

Articolul 4. Activitatea specială de investigaţii şi drepturile omului

(1) Orice persoană supusă măsurii speciale de investigaţii are dreptul să fie informată, după efectuarea acesteia, de către procuror sau de către judecătorul de instrucţie care a autorizat măsura dacă aceasta nu a atras dispunerea unei alte măsuri speciale de investigaţii.

(2) Orice persoană supusă măsurii speciale de investigaţii are dreptul la repararea prejudiciului material şi moral cauzat prin încălcarea prezentei legi.

(3) Înfăptuirea măsurii speciale de investigaţii pentru realizarea altor scopuri şi sarcini decît cele prevăzute de prezenta lege nu se admite.

(4) Activitatea specială de investigaţii exercitată cu încălcarea prezentei legi atrage răspunderea prevăzută de lege.

(5) Orice informaţie, orice probă care au fost acumulate cu încălcarea drepturilor şi libertăţilor omului sînt nule şi se consideră inexistente.

Articolul 5. Protecţia datelor cu caracter personal în procesul exercitării activităţii speciale de investigaţii

(1) Persoanele care au acces la datele cu caracter personal ale persoanei supuse măsurii speciale de investigaţii sînt obligate să păstreze confidenţialitatea datelor respective în conformitate cu prevederile Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

(2) Accesul la dosarul special sau la materialele din dosar al altor persoane decît cele care investighează dosarul special este interzis, cu excepţia conducătorului subdiviziunii specializate a organului respectiv, în limitele competenţei, şi a procurorului care a autorizat măsura specială de investigaţii sau a solicitat autorizarea acesteia de către judecătorul de instrucţie, precum şi cu excepţia judecătorului de instrucţie care a autorizat măsura specială de investigaţii.

Articolul 7. Competenţa autorităţilor ale căror subdiviziuni specializate efectuează activitatea specială de investigaţii

(1) În scopul organizării şi realizării activităţii speciale de investigaţii, autorităţile ale căror subdiviziuni specializate efectuează activitatea specială de investigaţii au competenţa de:

a) a crea sisteme informaţionale pentru a asigura realizarea sarcinilor activităţii speciale de investigaţii;

b) a încheia acorduri cu privire la folosirea încăperilor de serviciu, a locuinţelor, a mijloacelor de transport, a bunurilor întreprinderilor, instituţiilor, organizaţiilor, unităţilor militare, precum şi a altor bunuri ale persoanelor fizice şi juridice;

c) a confecţiona şi a folosi, în cadrul efectuării măsurilor speciale de investigaţii, acte care codifică identitatea persoanelor cu funcţii de răspundere, a subdiviziunilor, organizaţiilor, încăperilor şi mijloacelor de transport, precum şi identitatea colaboratorilor confidenţiali;

d) a achiziţiona mijloace tehnice speciale, cum ar fi: aparate de înregistrare video şi audio, de fotografiat, alte mijloace tehnice moderne pentru obţinerea în secret a informaţiei;

e) a înfiinţa, în modul stabilit de lege, întreprinderi, organizaţii şi subdiviziuni în vederea soluţionării sarcinilor prevăzute de prezenta lege.

(2) Competenţele specificate la alin.(1) lit.c) şi d) revin numai subdiviziunilor specializate ale Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie şi Serviciului de Informaţii şi Securitate al Republicii Moldova.

(3) Subdiviziunile specializate ale autorităţilor care efectuează activitatea specială de investigaţii, în limitele competenţei lor, au dreptul să colecteze informaţiile necesare ce caracterizează persoanele supuse verificării privind:

a) accesul la informaţiile ce constituie secret de stat;

b) admiterea la muncă la obiectivele care prezintă un pericol sporit pentru viaţa şi sănătatea oamenilor;

c) admiterea la organizarea şi desfăşurarea unor măsuri speciale de investigaţii sau accesul la materialele primite pe parcursul executării acestor măsuri;

d) stabilirea sau întreţinerea relaţiilor de colaborare la organizarea şi desfăşurarea măsurilor speciale de investigaţii;

e) examinarea de către organul de licenţiere a cererii de eliberare a licenţei pentru activitatea particulară de detectiv şi/sau de pază;

f) asigurarea securităţii interne

Articolul 15. Colaboratorii confidenţiali

(1) Colaboratorii confidenţiali sînt persoane care, printr-un acord scris sau verbal, se obligă să ofere ofiţerului de investigaţii informaţii, să participe la pregătirea şi efectuarea măsurilor speciale de investigaţii, precum şi să contribuie într-un alt mod, neinterzis de lege, la activităţile speciale de investigaţii.

(2) Antrenarea colaboratorilor confidenţiali la efectuarea măsurilor speciale de investigaţii poate fi realizată cu titlu oneros sau gratuit.

(3)Ofiţerii de investigaţii, după caz, pot încheia acorduri cu colaboratorii confidenţiali în numele autorităţii ale cărei subdiviziuni efectuează activitatea specială de investigaţii.

(4) Colaboratorii confidenţiali sînt obligaţi să păstreze secretul informaţiilor ce le-au devenit cunoscute în timpul efectuării măsurilor speciale de investigaţii şi să prezinte informaţii veridice.

(5) În scopul asigurării securităţii colaboratorilor confidenţiali, a membrilor familiilor şi a rudelor acestora, se permite efectuarea de măsuri speciale de investigaţii în vederea protecţiei lor în modul stabilit de lege. Informaţia despre colaboratorul confidenţial poate fi făcută publică doar cu acordul scris al acestuia.

(6) Ofiţerilor de investigaţii li se interzice să antreneze în activitatea specială de investigaţii, în calitate de colaboratori confidenţiali, deputaţi, judecători, procurori, ofiţeri de urmărire penală şi avocaţi. (7) Activitatea colaboratorilor confidenţiali se află sub controlul conducătorilor autorităţilor ale căror subdiviziuni efectuează activitatea specială de investigaţii şi al conducătorilor subdiviziunilor specializate respective.

Articolul 16. Asistenţa acordată subiecţilor activităţii speciale de investigaţii

(1) Persoanele fizice şi juridice, indiferent de forma de proprietate, sînt obligate să acorde asistenţă subdiviziunilor specializate, să pună imediat la dispoziţia acestora informaţiile solicitate, precum şi, în măsura posibilităţilor, bunuri mobile şi imobile, alte obiecte şi documente necesare pentru realizarea măsurilor speciale de investigaţii.

(2) Persoanele juridice prestatoare de servicii poştale şi de

comunicaţii electronice sînt obligate să asigure echipamentele şi condiţiile tehnice necesare pentru înfăptuirea de către subdiviziunile specializate a măsurilor speciale de investigaţii, precum şi să întreprindă acţiuni pentru păstrarea confidenţialităţii conţinutului, metodelor şi tacticii acestor măsuri.

Capitolul III
MĂSURILE SPECIALE DE INVESTIGAŢII
Secţiunea 1
Procedura de dispunere a măsurilor speciale de investigaţii

Articolul 18. Măsurile speciale de investigaţii

(1) Pentru realizarea sarcinilor prevăzute de prezenta lege pot fi efectuate următoarele măsuri speciale de investigaţii:

1) cu autorizarea judecătorul de instrucţie, la demersul procurorului:

a) cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat;

b) supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea;

c) interceptarea şi înregistrarea comunicărilor şi imaginilor;

d) reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale;

e) monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice;

f) monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară;

g) documentarea cu ajutorul metodelor şi mijloacelor tehnice, precum şi localizarea sau urmărirea prin sistem de poziţionare globală (GPS) ori prin alte mijloace tehnice;

h) colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice;

2) cu autorizarea procurorului:

a) identificarea abonatului, proprietarului sau a utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic;

b) urmărirea vizuală;

c) controlul transmiterii banilor sau a altor valori materiale extorcate;

d) investigaţia sub acoperire;

e) supravegherea transfrontalieră;

f) livrarea controlată;

g) colectarea mostrelor pentru cercetarea comparată;

h) cercetarea obiectelor şi documentelor;

i) achiziţia de control;

3) cu autorizarea conducătorului subdiviziunii specializate:

a) chestionarea;

b) culegerea informaţiei despre persoane şi fapte;

c) identificarea persoanei.

(2) Lista măsurilor specificate la alin.(1) este exhaustivă şi poate fi modificată sau completată doar prin lege.

(3) Măsurile prevăzute la alin.(1) pct.1), precum şi cele prevăzute la alin. (1) pct.2) lit.c), e), şi f) se efectuează numai în cadrul unui proces penal, conform Codului de procedură penală al Republicii Moldova. Celelalte măsuri prevăzute la alin.(1) pct.2) se efectuează atît în cadrul unui proces penal, cît şi în afara acestuia. Măsurile prevăzute la alin.(1) pct.3) se efectuează în afara procesului penal.

(31) Măsurile prevăzute la alin.(1) pct.1) lit.c), g) şi h), precum şi cele prevăzute la alin.(1) pct.2) pot fi efectuate în afara unui proces penal, în cadrul testului de integritate profesională, cu autorizarea judecătorului, în condiţiile Legii nr.325 din 23 decembrie 2013 privind evaluarea integrităţii instituţionale.

(4) Măsura specială de investigaţii prevăzută la alin.(1) pct.2) lit.c) se efectuează doar de către subdiviziunile specializate ale Ministerului Afacerilor Interne şi ale Centrului Naţional Anticorupţie.

(5) În procesul efectuării măsurilor speciale de investigaţii se face uz de sisteme informaţionale, de aparate de înregistrare video şi audio, de aparate de fotografiat şi de filmat, de alte mijloace tehnice, dacă acestea au fost autorizate în modul stabilit de lege.

(6) Organizarea, metodele efectuării măsurilor speciale de investigaţii, procedurile interne de autorizare, regulile de întocmire a proceselor-verbale cu privire la gestionarea, păstrarea şi distrugerea materialelor obţinute, măsurile de asigurare a integrităţii şi confidenţialităţii acestora şi a confidenţialităţii activităţilor speciale de investigaţii, regulile de înfăptuire a operaţiunilor sub acoperire şi cu privire la conducerea şi gestionarea activităţii efectuate sub acoperire, modul de înregistrare a dosarelor speciale, precum şi utilizarea resurselor financiare alocate pentru efectuarea măsurilor speciale de investigaţii, sînt stabilite printr-un regulament comun al autorităţilor care efectuează activitate specială de investigaţii de comun acord cu Procuratura Generală.

Articolul 23. Accesul la sistemele informaţionale

Ofiţerii de investigaţii, în limitele dosarului special, au acces gratuit , inclusiv prin intermediul platformei de interoperabilitate, la datele sistemelor informaţionale, cu excepţiile prevăzute de legile respective.

Articolul 25. Confidenţialitatea datelor cu privire la măsurile speciale de investigaţii

(1) Toate datele acumulate în timpul efectuării măsurii speciale de investigaţii constituie informaţie oficială cu accesibilitate limitată sau secret de stat.

(2) Orice divulgare a datelor specificate la alin.(1) atrage răspunderea prevăzută de lege.

PARLAMENTUL

LEGE *Nr. 269* din 12-12-2008

privind aplicarea testării la detectorul comportamentului simulat (poligraf)

Publicat : 20-03-2009 în Monitorul Oficial Nr. 57-58 art. 161

Versiune în vigoare din 15.06.18 în baza modificărilor prin LP79 din 24.06.18, MO195-209/15.06.18 art.338

Articolul 1. Noţiuni principale

În sensul prezentei legi, următoarele noţiuni principale semnifică:

detector al comportamentului simulat (denumit în continuare *poligraf*) – mijloc

tehnic de înregistrare a parametrilor fiziologici (inclusiv ai respiraţiei, ai activităţii cardio-vasculare, ai sensibilităţii chinestezice a pielii), care permite detectarea comportamentului simulat cu prezentarea rezultatelor înregistrate în formă analogă şi/sau digitală;

testare cu utilizarea poligrafului – totalitate de acţiuni netraumatizante, inofensive pentru viaţa şi sănătatea omului (incluzînd şi testarea la poligraf), orientate spre verificarea de către poligrafolog a veridicităţii informaţiilor comunicate de persoana testată;

testare la poligraf – parte componentă a testării cu utilizarea poligrafului, incluzînd înregistrarea parametrilor fiziologici ai omului ca răspuns la întrebările puse, la obiectele şi la imaginile prezentate;

poligrafolog – specialist, atestat în conformitate cu cerinţele prezentei legi, care testează la poligraf;

asistent al poligrafologului – persoană special instruită pentru a acorda asistenţă tehnică în timpul testării la poligraf;

persoană testată – persoană supusă testării cu utilizarea poligrafului;

iniţiator al testării – persoană juridică iniţiatoare a testării cu utilizarea poligrafului în cazurile prevăzute de prezenta lege;

testare obligatorie – testare a cărei efectuare este obligatorie pentru iniţiatorul testării şi pentru persoana testată, în cazurile stipulate în prezenta lege;

testare benevolă – testare efectuată cu consimţământul benevol al persoanei testate, în cazurile stipulate în prezenta lege;

factor de risc – temei, stabilit de iniţiatorul testării în conformitate cu principiile prezentei legi şi cu normele legislaţiei, pentru refuzul angajării ori pentru sistarea exercitării atribuţiilor de serviciu;

consimţământ al testării – decizie, fixată în formă scrisă, a persoanei de a fi testată cu utilizarea poligrafului în termenele propuse de iniţiatorul testării;

refuz al testării – decizie a persoanei de a nu accepta să fie testată cu utilizarea poligrafului, fixată în formă scrisă de această persoană sau de poligrafolog;

cerere de modificare a termenului testării cu utilizarea poligrafului – solicitare a persoanei, fixată în formă scrisă, privind modificarea termenului de testare în temeiurile prevăzute de prezenta lege;

rezultat al testării cu utilizarea poligrafului – aviz al specialistului poligrafolog întocmit în baza informaţiei obţinute de la persoana testată;

materiale ale testării – rezultatul testării, întrebările puse persoanei testate în timpul testării la poligraf şi reacţiile ei fiziologice înregistrate, înregistrările audio şi video ale interviului efectuat înainte de testare, ale testării la poligraf şi/sau ale interviului de după testare;

Comisia de stat pentru testări cu utilizarea poligrafului – autoritate coordonatoare abilitată cu stabilirea şi controlul respectării principiilor organizatorice ale efectuării testărilor cu utilizarea poligrafului, normelor metodice unice de efectuare a unor astfel de testări şi modului de pregătire a poligrafologilor.

Articolul 2. Scopurile testării cu utilizarea poligrafului şi domeniile ei de aplicare

(1) Testarea cu utilizarea poligrafului (denumită în continuare *testare*) se efectuează pentru evaluarea veridicităţii informaţiilor comunicate de persoana testată, în cazurile stabilite de prezenta lege.

(2) Evaluarea veridicităţii informaţiilor comunicate de persoana testată se efectuează:

a) la angajare în serviciu în cadrul instituţiilor menţionate la art.7;

b) la efectuarea controlului periodic sau selectiv al activităţii de serviciu în cadrul instituţiilor menţionate la art.7;

c) în cadrul anchetei de serviciu;

d) în cadrul activităţii operative de investigaţii.

Articolul 3. Principiile testării

(1) Testarea se efectuează cu respectarea drepturilor şi libertăţilor omului şi ale cetăţeanului, stabilite de Constituţia Republicii Moldova, în conformitate cu principiile legalităţii, umanismului, caracterului ştiinţific, confidenţialităţii, în cazurile prevăzute de prezenta lege.

(2) Testarea nu trebuie să prezinte pericol pentru sănătatea omului, nu trebuie să-i lezeze onoarea şi demnitatea.

(3) Este inadmisibilă recurgerea la ameninţări, la violenţă şi la măsuri de influenţă pentru a constrînge persoana să accepte testarea ori să fie astfel testată.

(4) Dreptul de iniţiere a testării se acordă Consiliului Superior al Magistraturii, Consiliului Superior al Procurorilor, organelor Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie, Autorităţii Naţionale de Integritate, Serviciului de Informaţii şi Securitate şi Serviciului Vamal. Testarea va fi efectuată de specialişti atestaţi în conformitate cu prezenta lege.

(5) Informaţia din materialele testării şi informaţia obţinută de participanţii la testare în cadrul acesteia nu pot fi divulgate fără consimţămîntul persoanei testate, cu excepţia cazurilor prevăzute de prezenta lege. Este inadmisibilă folosirea acestei informaţii în scopuri neprevăzute de prezenta lege.

Articolul 4. Persoanele supuse testării

În cazurile prevăzute de prezenta lege, persoanele – cetăţeni ai Republicii Moldova, cetăţeni străini sau apatrizi – vor fi supuse testării dacă:

a) se angajează sau îndeplinesc serviciul în cadrul organelor Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie, Autorităţii Naţionale de Integritate, Serviciului de Informaţii şi Securitate şi Serviciului Vamal;

a[1]) participă la concursul pentru numirea în funcţia de judecător sau de procuror;

a[2]) participă la concursul pentru numirea în funcţia de preşedinte sau vicepreşedinte al Autorităţii Naţionale de Integritate;

b) aceasta decurge din contractul de muncă;

c) aceasta decurge din activitatea operativă de investigaţii;

d) persoana doreşte benevol să fie supusă testării, în conformitate cu prezenta lege.

Articolul 22. Obligaţiile şi drepturile poligrafologului

(3) Poligrafologul nu are dreptul:

a) să efectueze testări în cazul existenţei temeiului indicat la art.6;

b) să adreseze în timpul testării întrebări ce ţin de apartenenţa rasială sau etnică a persoanei testate, de convingerile ei religioase sau politice, de viaţa şi orientarea ei sexuală, cu excepţia cazurilor cînd formularea unor astfel de întrebări ţine de efectuarea cercetărilor de către organele competente;

c) să adreseze în timpul testării întrebări care urmăresc obţinerea unor informaţii ce constituie secret de stat, cu excepţia cazurilor cînd formularea unor astfel de întrebări ţine de efectuarea cercetărilor de către organele competente;

d) să nu prezinte iniţiatorului testării informaţiile obţinute în timpul efectuării testării;

e) să expună în avizul său concluzii cu caracter juridic, medical, psihologic, psihiatric sau de alt gen în privinţa persoanei testate dacă nu este specialist în domeniul respectiv.

(4) Poligrafologul are dreptul:

a) să ia cunoştinţă de materialele de care dispune iniţiatorul testării, necesare pregătirii către testare, testării persoanei în a cărei privinţă a fost iniţiată testarea;

b) să refuze efectuarea testării în cazul în care iniţiatorul nu prezintă materialele menţionate la lit.a) sau în cazul insuficienţei timpului necesar pregătirii de lucru cu persoana testată.

PARLAMENTUL

COD *Nr. 122* din 14-03-2003

CODUL DE PROCEDURĂ PENALĂ AL REPUBLICII MOLDOVA

Publicat : 05-11-2013 în Monitorul Oficial Nr. 248-251 art. 699

MODIFICAT LP99 din 11.06.20, MO161-164/03.07.20 art.313; în vigoare 03.10.20

Articolul 14. Secretul corespondenţei

(1) Dreptul la secretul scrisorilor, al telegramelor, al altor trimiteri poştale, al convorbirilor telefonice şi al celorlalte mijloace legale de comunicare este asigurat de stat. În cursul procesului penal, nimeni nu poate fi lipsit sau limitat în acest drept.

(2) Limitarea dreptului prevăzut la alin.(1) se admite numai în baza unui mandat judiciar emis în condiţiile prezentului cod.

Articolul 15. Inviolabilitatea vieţii private

(1) Orice persoană are dreptul la inviolabilitatea vieţii private, la confidenţialitatea vieţii intime, familiale, la protejarea onoarei şi demnităţii personale. În cursul procesului penal, nimeni nu este în drept să se implice în mod arbitrar şi nelegitim în viaţa intimă a persoanei.

(2) La efectuarea acţiunilor procesuale nu poate fi acumulată fără necesitate informaţie despre viaţa privată şi intimă a persoanei. La cererea organului de urmărire penală şi a instanţei de judecată, participanţii la acţiunile procesuale sînt obligaţi să nu divulge asemenea informaţii şi despre aceasta se ia un angajament în scris. Prelucrarea datelor cu caracter personal în cadrul procesului penal se efectuează în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

(3) Persoanele de la care organul de urmărire penală cere informaţie despre viaţa privată şi intimă sînt în drept să se convingă că această informaţie se administrează într-o cauză penală concretă. Persoana nu este în drept să refuze de a prezenta informaţii despre viaţa privată şi intimă a sa sau a altor persoane sub pretextul inviolabilităţii vieţii private, însă ea este în drept să ceară de la organul de urmărire penală explicaţii asupra necesităţii obţinerii unei asemenea informaţii, cu includerea explicaţiilor în procesul-verbal al acţiunii procesuale respective.

(4) Probele care confirmă informaţia despre viaţa privată şi intimă a persoanei, la cererea acesteia, se examinează în şedinţă de judecată închisă.

(5) Prejudiciul cauzat persoanei în cursul procesului penal prin violarea vieţii private şi intime a acesteia se repară în modul stabilit de legislaţia în vigoare.

Articolul 54[1]. Consultantul procurorului

(1) În cadrul procesului penal, procurorul poate fi asistat de un consultant.

(4) Consultantul este obligat să păstreze secretul profesional, confidenţialitatea asupra faptelor şi informaţiilor care i-au devenit cunoscute în exercitarea atribuţiilor care îi revin şi poartă răspundere, conform legii, pentru acţiunile ilegale săvîrşite în exerciţiul funcţiei.

Articolul 82. Asistentul procedural

(1) Asistentul procedural este persoana care nu are interes personal în cauză, nu este angajat al organului de urmărire penală şi participă la prezentarea persoanei spre recunoaştere.

(3) Asistentul procedural este obligat:

6) să nu dea publicităţii circumstanţele şi datele ce i-au devenit cunoscute în urma efectuării acţiunii procesuale, inclusiv circumstanţele ce se referă la inviolabilitatea vieţii private, de familie, precum şi cele care constituie secret de stat, secret comercial sau alte informaţii oficiale cu accesibilitate limitată.

Articolul 85. Interpretul, traducătorul

(1) Interpret, traducător este persoana care cunoaşte limbile necesare pentru interpretarea semnelor celor muţi ori surzi sau traducere, precum şi terminologia juridică, nu este interesată în cauza penală şi acceptă să participe în această calitate. Interpretul, traducătorul este desemnat în această calitate de organul de urmărire penală sau de instanţa de judecată în cazurile prevăzute de prezentul cod. Interpretul, traducătorul poate fi numit din rîndul persoanelor propuse de către participanţii la procesul penal.

(4) Interpretul, traducătorul este obligat:

9) să nu divulge circumstanţele şi datele care i-au devenit cunoscute în urma efectuării acţiunii procesuale, inclusiv circumstanţele ce se referă la inviolabilitatea vieţii private, de familie, precum şi cele care constituie secret de stat, secret comercial sau alte informaţii oficiale cu accesibilitate limitată.

Articolul 87. Specialistul

(1) Specialistul este persoana chemată pentru a participa la efectuarea unei acţiuni procesuale în cazurile prevăzute de prezentul cod, care nu este interesată în rezultatele procesului penal. Cererea organului de urmărire penală,procurorului, organului de constatare sau a instanţei cu privire la chemarea specialistului este obligatorie pentru conducătorul întreprinderii, instituţiei sau organizaţiei în care activează specialistul.

(5) Specialistul este obligat:

10) să nu divulge circumstanţele şi datele care i-au devenit cunoscute în urma efectuării acţiunii procesuale, inclusiv circumstanţele ce se referă la inviolabilitatea vieţii private, de familie, precum şi cele care constituie secret de stat, secret comercial sau alte informaţii oficiale cu accesibilitate limitată.

Articolul 88. Expertul

(1) Expertul este persoana numită pentru a efectua investigaţii în cazurile prevăzute de prezentul cod, care nu este interesată în rezultatele cauzei penale şi care, aplicînd cunoştinţele speciale din domeniul ştiinţei, tehnicii, artei şi din alte domenii, prezintă rapoarte în baza acestora.

(3) Expertul este obligat:

9) să nu divulge circumstanţele şi datele ce i-au devenit cunoscute în urma efectuării expertizei judiciare sau în urma participării la şedinţa de judecată închisă, inclusiv circumstanţele ce se referă la inviolabilitatea vieţii private, de familie, precum cele care constituie secret de stat, secret comercial sau alte informaţii oficiale cu accesibilitate limitată;

Articolul 126. Temeiurile pentru ridicarea de obiecte sau documente

(1) Organul de urmărire penală, în baza unei ordonanţe motivate, este în drept să ridice obiectele sau documentele care au importanţă pentru cauza penală dacă probele acumulate sau materialele activităţii speciale de investigaţii indică exact locul şi persoana la care se află acestea.

(2) Ridicarea de documente ce conţin informaţii care constituie secret de stat, comercial, bancar, precum şi ridicarea informaţiei privind convorbirile telefonice se fac numai cu autorizaţia judecătorului de instrucţie.

Articolul 128. Procedura efectuării percheziţiei sau ridicării de obiecte şi documente

(5) În cadrul efectuării percheziţiei, după prezentarea ordonanţei, reprezentantul organului de urmărire penală cere să i se predea obiectele şi documente-

le menţionate în ordonanţă. Instituţiile financiare nu pot invoca secretul bancar drept motiv pentru a refuza prezentarea documentelor solicitate. Dacă obiectele şi documentele căutate se predau benevol, persoana care efectuează urmărirea penală se limitează la ridicarea acestora, fără a mai efectua alte măsuri de investigaţii.

Articolul 132[6]. Cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat

(1) Cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat presupune accesul secret sau legendat în interiorul domiciliului, fără înştiinţarea proprietarului, posesorului, în scopul studierii acestuia pentru descoperirea urmelor activităţii infracţionale, persoanelor aflate în căutare, pentru obţinerea altor informaţii necesare probării circumstanţelor faptei, precum şi pentru observarea şi înregistrarea evenimentelor care se produc în domiciliu.

(2) Cercetînd domiciliul, ofiţerul de investigaţii examinează obiectele vizibile şi, cu autorizarea judecătorului de instrucţie, poate instala în acesta aparate de înregistrare audio şi video, de fotografiat, de filmat sau alte mijloace tehnice care asigură interceptarea şi înregistrarea de la distanţă a informaţiei sau înregistrarea ei nemijlocită în domiciliu.

(3) Cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat se dispune cu privire la persoana asupra căreia există probe sau date că a săvîrşit sau pregăteşte săvîrşirea unei infracţiuni. Cercetarea domiciliului şi instalarea în el a aparatelor audio şi video, a celor de fotografiat şi de filmat se pot dispune şi cu privire la o altă persoană dacă există o bănuială rezonabilă că aceasta primeşte sau transmite comunicări de la făptuitor ori destinate acestuia.

(4) La cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat se întocmeşte un proces-verbal conform prevederilor prezentului cod.

(5) Supravegherea şi înregistrarea audio şi video, fotografierea şi filmarea se dispun pe o perioadă de 30 de zile, cu posibilitatea prelungirii pînă la 3 luni, însă nu mai mult de durata urmăririi penale.

Articolul 132[7]. Supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea

(1) Supravegherea domiciliului prin utilizarea mijloacelor tehnice de înregistrare audio sau video presupune monitorizarea domiciliului din exterior, fără

acordul proprietarului sau posesorului, dacă există temeiuri de a considera că acţiunile, convorbirile, alte sunete sau evenimente ce se produc în acel domiciliu pot conţine informaţii despre circumstanţele faptei care urmează a fi probate.

(2) Supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea se dispune pe o perioadă de 30 de zile, cu posibilitatea prelungirii pînă la 3 luni, însă nu mai mult de durata urmăririi penale.

Articolul 132[8]. Interceptarea şi înregistrarea comunicărilor

(1) Interceptarea şi înregistrarea comunicărilor presupun folosirea unor mijloace tehnice prin intermediul cărora se poate afla conţinutul unor convorbiri între două sau mai multe persoane, iar înregistrarea acestora presupune stocarea informaţiilor obţinute în urma interceptării pe un suport tehnic.

(2) Prevederile alin. (1) se aplică în exclusivitate la cauzele penale care au ca obiect urmărirea penală sau judecarea persoanelor asupra cărora există date sau probe cu privire la săvîrşirea infracţiunilor prevăzute în următoarele articole din Codul penal: art. 135–145, 150, 151, 158, 164–165[1], art. 166 alin. (2) şi (3), art. 166[1], 167, art. 171 alin. (2) şi (3), art. 172 alin. (2) şi (3), art. 175, 175[1], art. 186 alin. (3)–(5), art. 187 alin. (3)–(5), art. 188, 189, art. 190 alin. (3)–(5), art. 191 alin. (2) lit. d) şi alin. (3)–(5), art. 192[1]alin. (3), art. 201[1]alin. (3), art. 206, 207, 208[1], 208[2], art. 216 alin. (3), art. 217 alin. (3), art. 217[1] alin. (3) şi (4), art. 217[3] alin. (3), art. 217[4] alin. (2) şi (3), art. 219 alin. (2), art. 220 alin. (2) şi (3), art. 224 alin. (3) şi (4), art. 236, 237, art. 241[1] alin. (2), art. 242[1]–243, art. 244 alin. (2), art. 248 alin. (2)–(5), art. 259–261[1], 275, 278–279[1], art. 279[2] alin. (3) lit. b), art. 279[3], art. 280, 282–286, 289–289[3], art. 290 alin. (2), art. 292, 295–295[2], art. 303 alin. (3), art. 306–309, 318, 324–328, 333–335, art. 335[1] alin. (2), art. 337–340, 342–344, art. 352 alin. (3), art. 362, 362[1], art. 368 alin. (2), art. 370 alin. (2) şi (3). Lista componentelor de infracţiuni este exhaustivă şi poate fi modificată doar prin lege.

(3) Pot fi supuse interceptării şi înregistrării comunicările bănuitului, învinuitului sau ale altor persoane, inclusiv ale celor a căror identitate nu a fost stabilită, despre care există date ce pot conduce rezonabil la concluzia că ele fie contribuie, în orice mod, la pregătirea, comiterea, favorizarea sau tăinuirea infracţiunilor prevăzute la alin. (2), fie primesc sau transmit informaţii relevante şi importante pentru cauza penală.

(4) Pot fi supuse interceptării şi înregistrării comunicările victimei, părţii vătămate, ale rudelor şi ale membrilor familiei sale, precum şi ale martorului, dacă există pericol iminent pentru viaţa, sănătatea sau pentru alte drepturi fundamentale ale acesteia, dacă este necesară prevenirea infracţiunii sau dacă există riscul evident al pierderii iremediabile sau al denaturării probelor. Interceptarea şi înre-

gistrarea comunicărilor în sensul prezentului alineat se dispune conform procedurii prevăzute la art. 132[4]şi doar cu acordul în scris sau la cererea prealabilă în scris a persoanelor indicate în prezentul alineat. Măsura dispusă conform prezentului alineat urmează a fi încetată imediat după dispariţia temeiului care a stat la baza autorizării acesteia sau la cererea expresă a persoanei în privinţa căreia a fost dispusă măsura.

Articolul 132[9]. Efectuarea şi certificarea interceptării şi înregistrării comunicărilor

(1) Interceptarea şi înregistrarea comunicărilor se efectuează de către organul de urmărire penală sau de către ofiţerul de investigaţii. Asigurarea tehnică a interceptării comunicărilor se realizează de către autoritatea abilitată prin lege cu asemenea atribuţii, utilizîndu-se mijloace tehnice speciale. Colaboratorii subdiviziunii din cadrul instituţiei autorizate prin lege, care asigură tehnic interceptarea şi înregistrarea comunicărilor, precum şi persoanele care efectuează nemijlocit ascultarea înregistrărilor, ofiţerii de urmărire penală şi procurorul sînt obligaţi să păstreze secretul comunicărilor şi poartă răspundere pentru încălcarea acestei obligaţii.

(2) Pentru asigurarea interceptării şi înregistrării comunicărilor, organul de urmărire penală sau procurorul prezintă organului abilitat prin lege extrasul din încheierea judecătorului de instrucţie, autentificat de către acesta, privind dispunerea efectuării interceptării comunicărilor. Scrisoarea de însoţire a extrasului din încheierea judecătorului de instrucţie va conţine o menţiune privind preîntîmpinarea persoanei care va asigura tehnic efectuarea măsurii speciale de investigaţii despre răspunderea penală. Extrasul din încheiere trebuie să conţină denumirea instanţei şi numele judecătorului de instrucţie, data şi ora emiterii încheierii, datele privind examinarea demersului procurorului pentru autorizarea efectuării măsurii, datele de identificare ale abonatului sau ale unităţii tehnice prin intermediul căreia se poartă comunicările ce urmează a fi interceptate, durata interceptării, persoana sau organul de urmărire penală responsabil de executarea încheierii, semnătura judecătorului de instrucţie şi ştampila instanţei de judecată.

(3) În cazul în care în procesul interceptării şi înregistrării comunicărilor poate fi obţinută şi altă informaţie, cum ar fi date de identificare ale abonaţilor sau persoanelor care au purtat comunicări cu subiectul interceptării şi localizarea acestora, precum şi alte date, judecătorul de instrucţie poate dispune în încheierea de efectuare a interceptării comunicărilor şi obţinerea acestor informaţii.

(4) Subdiviziunea tehnică a organului abilitat prin lege să efectueze interceptarea şi înregistrarea comunicărilor transmite organului de urmărire penală semnalul comunicărilor interceptate şi alte informaţii indicate în extrasul din încheie-

rea judecătorului de instrucţie în regim de timp real, fără a efectua înregistrarea acestora.

(5) Informaţia obţinută în procesul interceptării şi înregistrării comunicărilor poate fi ascultată şi vizualizată în regim de timp real de către organul de urmărire penală şi procuror.

(6) Informaţia obţinută în procesul interceptării şi înregistrării comunicărilor se transmite, de către subdiviziunea tehnică care a efectuat interceptarea comunicărilor, ofiţerului de urmărire penală sau procurorului pe purtător material de informaţii împachetat, sigilat cu ştampila subdiviziunii tehnice şi cu indicarea numărului de ordine al purtătorului material.

(7) În termen de 24 de ore după expirarea termenului de autorizare a interceptării, organul de urmărire penală sau, după caz, procurorul întocmeşte la finele fiecărei perioade de autorizare, un proces-verbal privind interceptarea şi înregistrarea comunicărilor.

(8) Procesul-verbal privind interceptarea şi înregistrarea comunicărilor trebuie să conţină: data, locul şi ora întocmirii, funcţia persoanei care a efectuat măsura specială de investigaţii, numărul cauzei penale în cadrul căreia s-a efectuat măsura specială, menţiunea cu privire la ordonanţa procurorului şi încheierea judecătorului de instrucţie privind autorizarea măsurii speciale, datele de identitate şi de identificare tehnică ale subiectului ale cărui comunicări au fost interceptate şi înregistrate, perioada în care s-a efectuat interceptarea comunicărilor, menţiunea privind utilizarea mijloacelor tehnice, alte informaţii relevante obţinute în urma interceptării şi înregistrării comunicărilor referitoare la identificarea şi/sau localizarea unor subiecţi, cantitatea şi numărul de identificare al purtătorilor materiali pe care a fost înregistrată informaţia, numărul de comunicări stenografiate. La procesul-verbal se anexează stenograma comunicărilor care au importanţă pentru cauza penală.

(9) Stenograma comunicărilor constituie reproducerea integrală, în formă scrisă, pe suport de hîrtie, a comunicărilor interceptate şi înregistrate care au importanţă pentru cauza penală. În stenograma comunicărilor se indică data, ora şi durata comunicării, numele persoanelor, dacă sînt cunoscute, ale căror comunicări sînt stenografiate, precum şi alte date. Se interzice stenografierea comunicărilor dintre avocat şi persoana pe care o apără. Fiecare pagină a procesului-verbal de interceptare şi a stenogramei se semnează de către persoana care le-a întocmit. La procesul-verbal se anexează în original suportul pe care au fost înregistrate comunicările interceptate, făcîndu-se menţiune despre împachetarea şi sigilarea acestuia.

(10) Comunicările interceptate şi înregistrate se redau în limba în care a avut

loc comunicarea. În cazul în care comunicarea a avut loc într-o altă limbă decît cea de stat, comunicarea se traduce în limba în care se desfăşoară procesul penal de către un traducător autorizat.

(11) La sfîrşitul perioadei autorizate pentru interceptarea şi înregistrarea comunicării, organul de urmărire penală prezintă procurorului procesul-verbal al interceptării şi suportul în original pe care a fost înregistrată informaţia.

(12) Procurorul, după verificarea corespunderii conţinutului procesului-verbal şi a stenogramelor cu conţinutul înregistrărilor, prin ordonanţă, decide asupra pertinenţei acestora pentru cauza penală şi dispune care comunicări urmează a fi transcrise pe un suport aparte.

(13) Comunicările interceptate şi înregistrate se vor păstra integral pe suportul iniţial prezentat organului de urmărire penală de către subdiviziunea tehnică. Acest suport se va păstra la judecătorul de instrucţie care a autorizat măsura specială de investigaţii.

(14) Comunicările interceptate şi înregistrate care au fost stenografiate de către organul de urmărire penală şi au fost apreciate de către procuror ca fiind pertinente pentru cauza penală se transcriu de către subdiviziunea tehnică din cadrul organului de urmărire penală pe un suport aparte, care se anexează la materialele cauzei penale şi se păstrează la procurorul care conduce urmărirea penală.

(15) În termen de 48 de ore de la finisarea perioadei de autorizare a interceptării şi înregistrării, procurorul prezintă judecătorului de instrucţie procesul-verbal şi suportul în original pe care au fost înregistrate comunicările. Judecătorul de instrucţie se expune printr-o încheiere asupra respectării cerinţelor legale la interceptarea şi înregistrarea comunicărilor de către organul de urmărire penală şi decide care din comunicările înregistrate urmează a fi nimicite, desemnînd persoanele responsabile de nimicire. Nimicirea informaţiilor în baza încheierii judecătorului de instrucţie este consemnată de către persoana responsabilă într-un proces-verbal, care se anexează la cauza penală.

Articolul 132[10]. Înregistrările de imagini

Înregistrările de imagini se efectuează în condiţiile şi în modalităţile de interceptare şi înregistrare a comunicărilor prevăzute la art. 13[28] şi 132[9], care se aplică în mod corespunzător.

Articolul 132[11]. Verificarea înregistrării interceptărilor

Mijloacele de probă dobîndite în condiţiile art.132[8]–132[10] pot fi verificate prin constatare tehnico-ştiinţifică sau, după caz, prin expertiză judiciară dispusă de către instanţa de judecată la cererea părţilor sau din oficiu.

Articolul 133. Reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale

(1) Dacă există temeiuri rezonabile de a presupune că trimiterile poştale primite sau expediate de către bănuit, învinuit pot conţine informaţii ce ar avea importanţă probatorie în cauza penală pe una sau mai multe infracţiuni grave, deosebit de grave sau excepţional de grave şi dacă prin alte procedee probatorii nu pot fi obţinute probe, organul de urmărire penală este în drept să reţină, să cerceteze, să predea, să percheziţioneze sau să ridice trimiterile poştale ale persoanelor indicate.

(2) Pot fi reţinute, cercetate, predate, percheziţionate sau ridicate următoarele trimiteri poştale: scrisori de orice gen, telegrame, radiograme, banderole, colete, containere poştale, mandate poştale, comunicări prin fax şi prin poşta electronică.

(3) Procurorul care conduce sau efectuează urmărirea penală întocmeşte o ordonanţă despre reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale, pe care o prezintă judecătorului de instrucţie. În ordonanţă trebuie să fie indicate: motivele dispunerii reţinerii, cercetării, predării, percheziţionării sau ridicării trimiterilor poştale, denumirea instituţiei poştale asupra căreia se pune obligaţia de a reţine trimiterile poştale, numele şi prenumele persoanei sau persoanelor ale căror trimiteri poştale trebuie să fie reţinute, adresa exactă a acestor persoane, genul de trimiteri poştale care se reţin, se cercetează, se predau, se percheziţionează sau se ridică şi durata măsurii. Durata de autorizare a măsurii se prelungeşte în condiţiile prezentului cod.

(4) Ordonanţa cu privire la reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale cu autorizaţia respectivă se transmite şefului instituţiei poştale, pentru care executarea acestei ordonanţe este obligatorie.

(5) Şeful instituţiei poştale comunică imediat organului care a emis ordonanţa reţinerea trimiterilor poştale indicate în aceasta.

(6) Reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale se anulează de către organul de urmărire penală care a emis ordonanţa respectivă, de către procurorul ierarhic superior, de către judecătorul de instrucţie după expirarea termenului pentru care a fost emisă autorizaţia, dar nu mai tîrziu de terminarea urmăririi penale.

Articolul 134. Examinarea şi ridicarea trimiterilor poştale

(1) Prezentîndu-se în instituţia poştală, reprezentantul organului de urmărire penală aduce la cunoştinţă şefului acestei instituţii, contra semnătură, ordonanţa de examinare şi ridicare a trimiterilor poştale, deschide şi examinează trimiterile poştale.

(2) La descoperirea de documente şi obiecte care au importanţă probatorie în cauza penală, reprezentantul organului de urmărire penală le ridică sau face copiile respective. În lipsa unor asemenea documente şi obiecte, reprezentantul organului de urmărire penală dispune înmînarea trimiterilor poştale examinate adresantului.

(3) Despre fiecare examinare şi ridicare a trimiterilor poştale se întocmeşte un proces-verbal conform prevederilor art. 260 şi 261, în care, în particular, se indică de către cine, unde, cînd a fost examinată, ridicată trimiterea poştală sau dispusă înmînarea acesteia adresantului, genul de trimitere poştală, precum şi de pe care trimiteri poştale au fost făcute copii, ce mijloace tehnice au fost utilizate şi ce s-a depistat. Toţi participanţii şi cei prezenţi la această acţiune procesuală sînt preveniţi despre obligativitatea păstrării secretului corespondenţei, nedivulgării informaţiei cu privire la urmărirea penală, precum şi despre răspunderea penală prevăzută la art. 178 şi 315 din Codul penal. Aceasta se consemnează în procesul-verbal.

Articolul 134[1]. Monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice

(1) Monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice şi a altor comunicări constă în accesul şi verificarea fără înştiinţarea expeditorului sau destinatarului a comunicărilor ce au fost transmise instituţiilor care prestează servicii de livrare a corespondenţei electronice sau a altor comunicări şi a apelurilor de primire şi ieşire ale abonatului.

(2) Monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice se dispune dacă sînt temeiuri verosimile de a presupune că acestea conţin sau pot conţine informaţii despre circumstanţele faptei care urmează a fi probate.

(3) Instituţiile care prestează servicii de livrare a corespondenţei electronice, a apelurilor de intrare şi ieşire sau a altor comunicări informează ofiţerul de urmărire penală sau procurorul despre aflarea în posesia lor a comunicărilor ce urmează a fi supuse verificării. Ofiţerul de urmărire penală sau procurorul ia cunoştinţă imediat, dar nu mai tîrziu de 48 de ore din momentul recepţionării informaţiei, de conţinutul comunicării şi adoptă o decizie privind ridicarea acesteia sau transmiterea ei pentru livrare ulterioară, cu fotografierea, copierea sau fixarea prin alt mijloc tehnic a conţinutului comunicării.

(4) Ridicarea conexiunilor se va efectua în cazul în care există temei de a considera că pentru procesul de administrare a probelor originalul va avea o importanţă mai mare decît copia sau fixarea vizuală.

Articolul 134[2]. Monitorizarea sau controlul tranzacţiilor financiare şi accesul

la informaţi financiară

(1) Monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară reprezintă operaţiunile prin care se asigură cunoaşterea conţinutului tranzacţiilor financiare efectuate prin intermediul instituţiilor financiare sau al altor instituţii competente ori obţinerea de la instituţiile financiare a înscrisurilor sau informaţiilor aflate în posesia acestora referitoare la depunerile, conturile sau tranzacţiile unei persoane.

(2) Monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară se dispun în cazul urmăririi penale pornite pe infracţiunile prevăzute la art. 158, 165, 165[1], 189–192, 196, 199, 206, 208, 209, 217–217[5], 220, 236, 237, 239–248, 251–253, 255, 256, 278, 279, 279[1], 279[3], 283, 284, 290, 292, 301[1], 302, 324–327, 330[1], 333, 334, 343, 352, 361 şi 362[1] din Codul penal.

Articolul 134[3]. Documentarea cu ajutorul metodelor şi mijloacelor tehnice, localizarea sau urmărirea prin sistemul de poziţionare globală (GPS) ori prin alte mijloace tehnice

(1) Documentarea cu ajutorul metodelor şi mijloacelor tehnice, precum şi localizarea sau urmărirea prin sistemul de poziţionare globală (GPS) ori prin alte mijloace tehnice reprezintă relevarea şi fixarea acţiunilor persoanelor, a unor imobile, a mijloacelor de transport şi a altor obiecte utilizînd aparate tehnice de înregistrare.

(2) La localizarea sau urmărirea prin sistemul de poziţionare globală (GPS) ori prin alte mijloace tehnice se pot folosi dispozitive care determină locul unde se află persoana sau obiectul utilizat de aceasta.

Articolul 134[4]. Colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice

Colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice şi a traficului de date computerizate constă în colectarea de la instituţiile de telecomunicaţii, de la operatorii de telefonie fixă sau mobilă, de la operatorii de internet a informaţiilor transmise prin canale tehnice de telecomunicaţii (telegraf, fax, paging, computer, radio şi alte canale), fixarea secretă a informaţiilor transmise sau primite prin intermediul liniilor tehnice de legături de telecomunicaţii de către persoanele supuse măsurii speciale de investigaţii, precum şi obţinerea de la operatori a informaţiei deţinute despre utilizatorii serviciilor de telecomunicaţii, inclusiv de roaming, şi despre serviciile de telecomunicaţii prestate acestora, la care se atribuie:

1) posesorii numerelor de telefon;

2) numerele de telefon înregistrate pe numele unei persoane;

3) serviciile de telecomunicaţii prestate utilizatorului;

4) sursa de comunicaţii (numărul de telefon al apelantului; numele, prenumele şi domiciliul abonatului sau utilizatorului înregistrat);

5) destinaţia comunicaţiei (numărul de telefon al apelatului sau numărul la care apelul a fost rutat, redirecţionat; numele, prenumele, domiciliul abonatului sau utilizatorului respectiv);

6) tipul, data, ora şi durata comunicaţiei, inclusiv tentativele de apel eşuate;

7) echipamentul de comunicaţii al utilizatorului sau alt dispozitiv utilizat pentru comunicaţie (imei al telefonului mobil, denumirea locaţiei Cell ID);

8) locul aflării echipamentului mobil de comunicaţii de la începutul comunicaţiei, locaţia geografică a celulei.

Articolul 134[5]. Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic

(1) Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic constă în solicitarea de la un furnizor de servicii electronice de a identifica abonatul, proprietarul sau utilizatorul unui sistem de telecomunicaţii, al unui mijloc de telecomunicaţii ori al unui punct de acces la un sistem informatic sau de a comunica dacă un anumit mijloc de comunicaţii sau punct de acces la un sistem informatic este folosit sau este activ ori a fost folosit sau a fost activ la o anumită dată.

(2) Ordonanţa de dispunere a măsurii speciale de investigaţii, pe lîngă elementele prevăzute la art. 255, va mai conţine:

1) datele de identificare ale furnizorului de servicii care dispune de datele specificate la alin. (1) sau le ţine la control;

2) datele de identificare ale abonatului, proprietarului sau utilizatorului, dacă sînt cunoscute; motivarea îndeplinirii condiţiilor de dispunere a măsurii speciale de investigaţii;

3) menţiunea cu privire la obligaţia persoanei sau a furnizorului de servicii de a comunica imediat, în condiţii de confidenţialitate, informaţiile solicitate.

(3) Furnizorii de servicii sînt obligaţi să colaboreze cu organele de urmărire penală pentru executarea ordonanţei procurorului şi să pună de îndată la dispoziţia acestora informaţiile solicitate.

(4) Persoanele care sînt chemate să colaboreze cu organele de urmărire penală au obligaţia de a păstra secretul operaţiunii efectuate. Încălcarea acestei obligaţii este pedepsită conform Codului penal.

Articolul 137. Activitatea şi măsurile de protecţie a investigatorului sub acoperire

(1) Investigatorul sub acoperire îşi desfăşoară activitatea în conformitate cu scopurile şi sarcinile indicate în ordonanţa procurorului.

(2) În procesul activităţilor desfăşurate, investigatorul sub acoperire efectuează măsurile speciale de investigaţii autorizate în funcţie de situaţia creată şi conform convingerii personale.

(3) Identitatea investigatorului sub acoperire este cunoscută numai procurorului şi poate fi dezvăluită numai cu acordul scris al investigatorului şi în conformitate cu Legea cu privire la secretul de stat.

Articolul 211. Păstrarea dosarelor penale şi a materialelor de urmărire penală

(1) Dosarele penale şi materialele de urmărire penală se păstrează la arhivele instanţelor judecătoreşti care au judecat cauza în primă instanţă.

(2) Dosarele penale şi materialele de urmărire penală care nu sînt înaintate în instanţa judecătorească se păstrează în arhiva organului care le-a întocmit.

(3) Dosarele penale şi materialele de urmărire penală care conţin secret de stat se păstrează în arhivele instituţiilor menţionate în alin.(1) şi (2), în condiţii speciale prevăzute de legislaţia în vigoare.

(4) Accesul la dosarele şi materialele care se păstrează în condiţiile prevăzute de prezentul articol se decide de către conducătorul organului sau, după caz, preşedintele instanţei la care se păstrează acestea, cu respectarea prevederilor prezentului capitol şi ale Legii nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

Articolul 212. Confidenţialitatea urmăririi penale

(1) Materialele urmăririi penale nu pot fi date publicităţii decît cu autorizaţia persoanei care efectuează urmărirea penală şi numai în măsura în care ea consideră că aceasta este posibil, cu respectarea prezumţiei de nevinovăţie, şi ca să nu fie afectate interesele altor persoane şi ale desfăşurării urmăririi penale în condiţiile Legii nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

(2) Dacă este necesar a se păstra confidenţialitatea, persoana care efectuează urmărirea penală previne martorii, partea vătămată, partea civilă, partea civil-

mente responsabilă sau reprezentanţii lor, apărătorul, expertul, specialistul, interpretul, traducătorul şi alte persoane care asistă la efectuarea acţiunilor de urmărire penală despre faptul că nu au voie să divulge informaţia privind urmărirea penală. Aceste persoane vor da o declaraţie în scris că au fost prevenite despre răspunderea pe care o vor purta conform art.315 din Codul penal.

(3) Divulgarea datelor urmăririi penale de către persoana care efectuează urmărirea penală sau de către persoana abilitată cu controlul asupra activităţii de urmărire penală, dacă această acţiune a cauzat daune morale sau materiale martorului, părţii vătămate şi reprezentanţilor acestora sau a prejudiciat procesul de urmărire penală, are ca urmare răspunderea penală prevăzută în art.315 din Codul penal.

Articolul 213. Apărarea secretului de stat în procesul penal

(1) În cursul procesului penal, pentru apărarea informaţiei ce constituie secret de stat se întreprind măsurile prevăzute de prezentul cod, de Legea cu privire la secretul de stat şi de alte acte normative.

(2) Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte date care constituie secret de stat au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte date ce constituie secret de stat nu pot refuza îndeplinirea acestei cerinţe, motivînd prin necesitatea păstrării secretului de stat, însă au dreptul să primească în prealabil de la persoana care efectuează urmărirea penală sau de la instanţă o explicaţie care ar confirma necesitatea furnizării datelor menţionate, cu includerea acestei explicaţii în procesul-verbal al acţiunii procesuale respective.

(3) Funcţionarul public care a făcut declaraţii privitor la datele ce îi sînt încredinţate şi ce constituie secret de stat comunică în scris despre acest fapt conducătorului organului de stat care dispune de această informaţie dacă comunicarea nu îi va fi interzisă în scris de către organul de urmărire penală sau instanţă.

(4) Efectuarea urmăririi penale sau judecarea cazului în cauzele legate de informaţia ce constituie secret de stat se încredinţează numai persoanelor care au dat în scris declaraţie de nedivulgare a unor asemenea informaţii. Declaraţia de nedivulgare se ia de către conducătorul organului de urmărire penală sau preşedintele instanţei şi se anexează la dosarul penal respectiv.

(5) Apărătorii şi alţi reprezentanţi, precum şi alte persoane cărora, în conformitate cu normele de procedură penală, le vor fi prezentate spre a lua act sau comunicate în alt mod date ce constituie secret de stat vor da în prealabil în scris

o declaraţie de nedivulgare a acestor date. În cazul în care apărătorul sau un alt reprezentant, cu excepţia reprezentantului legal, refuză să dea o astfel de declaraţie, acesta este lipsit de dreptul de a participa la procesul penal în cauză, iar celelalte persoane nu vor avea acces la datele ce constituie secret de stat. Declaraţia de nedivulgare de la persoanele menţionate în prezentul alineat se ia de către persoana care efectuează urmărirea penală sau instanţă şi se anexează la dosarul penal respectiv. Obligaţia de nedivulgare asumată de către participanţii la proces nu îi împiedică să ceară examinarea datelor ce constituie secret de stat în şedinţă de judecată închisă.

Articolul 214. Păstrarea secretului comercial şi a altor informaţii oficiale cu accesibilitate limitată

(1) În cursul procesului penal, pentru apărarea informaţiei ce constituie secret comercial sau a altor informaţii oficiale cu accesibilitate limitată se întreprind măsurile prevăzute de prezentul cod, de Legea cu privire la secretul comercial şi de alte acte normative.

(2) În cursul procesului penal nu pot fi administrate, utilizate şi răspîndite fără necesitate informaţii ce constituie secret comercial sau altă informaţie oficială cu accesibilitate limitată.

(3) Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte date care constituie secret comercial sau altă informaţie oficială cu accesibilitate limitată au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte date ce constituie secret comercial sau altă informaţie oficială cu accesibilitate limitată nu pot refuza îndeplinirea acestei cerinţe, motivînd prin necesitatea păstrării secretului, însă au dreptul să primească în prealabil de la persoana care solicită informaţii o explicaţie în scris care ar confirma necesitatea furnizării datelor menţionate.

(4) Funcţionarul public, angajatul întreprinderii sau al organizaţiei, indiferent de forma de proprietate, care a făcut declaraţii privitor la datele ce îi sînt încredinţate şi ce constituie secret comercial sau altă informaţie oficială cu accesibilitate limitată comunică acest fapt conducătorului unităţii respective, dacă comunicarea nu îi va fi interzisă în scris de organul de urmărire penală sau instanţă.

(5) Probele care dezvăluie informaţia ce constituie secret comercial sau altă informaţie oficială cu accesibilitate limitată, la solicitarea părţilor, se examinează în şedinţă de judecată închisă.

Articolul 293. Prezentarea materialelor de urmărire penală

(1) După verificarea de către procuror a materialelor cauzei şi adoptarea uneia din soluţiile prevăzute în art.291, procurorul aduce la cunoştinţă învinuitului, reprezentantului lui legal, apărătorului, părţii vătămate, părţii civile, părţii civilmente responsabile şi reprezentanţilor lor despre terminarea urmăririi penale, locul şi termenul în care ei pot lua cunoştinţă de materialele urmăririi penale. Părţii civile, părţii civilmente responsabile şi reprezentanţilor lor li se prezintă pentru a lua cunoştinţă doar materialele referitoare la acţiunea civilă la care sînt parte.

(2) Materialele urmăririi penale se aduc la cunoştinţa învinuitului arestat în prezenţa apărătorului lui, iar la cererea învinuitului – fiecăruia dintre ei, în mod separat.

(3) Pentru a se lua cunoştinţă de materialele urmăririi penale, ele se prezintă cusute în dosar, numerotate şi înscrise în borderou. La cererea părţilor, vor fi prezentate şi corpurile delicte, vor fi reproduse înregistrările audio şi video, cu excepţia cazurilor prevăzute în art.110. Dacă dosarul penal are mai multe volume, acestea se prezintă concomitent pentru a se lua cunoştinţă de materialele respective ca persoana care ia cunoştinţă de ele să poată reveni la oricare din aceste volume de mai multe ori. Pentru a se lua cunoştinţă de dosarele voluminoase, procurorul, printr-o ordonanţă, poate întocmi un grafic, coordonat cu apărătorul, prin care stabileşte data şi numărul volumelor pentru studiere.

(4) Termenul pentru a se lua cunoştinţă de materialele urmăririi penale nu poate fi limitat, însă în cazul în care persoana care ia cunoştinţă de materiale abuzează de situaţia sa, procurorul fixează modul şi termenul acestei acţiuni, reieşind din volumul dosarului.

(5) În scopul asigurării păstrării secretului de stat, comercial sau altor informaţii oficiale cu accesibilitate limitată, precum şi în scopul asigurării protecţiei vieţii, integrităţii corporale şi libertăţii martorului şi a altor persoane, judecătorul de instrucţie, conform demersului procurorului, poate limita dreptul persoanelor menţionate la alin.(1) de a lua cunoştinţă de materialele sau datele privind identitatea acestora. Demersul se examinează în condiţii de confidenţialitate, conform art. 305.

PARLAMENTUL

LEGE *Nr. 216* din 29-05-2003

cu privire la Sistemul informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni

Publicat : 08-08-2003 în Monitorul Oficial Nr. 170-172 art. 695

Versiune în vigoare din data 12.01.19 în baza modificărilor prin LP245 din15.11.18 MO 462-466 din12.12.18 art. 774

Articolul 1. Obiectul prezentei legi

Prezenta lege stabileşte principalele reguli şi condiţii de creare şi funcţionare a Sistemului informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni, drepturile şi obligaţiile participanţilor la el.

Articolul 2. Noţiuni de bază

În sensul prezentei legi, noţiunile utilizate semnifică:

Sistem informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni (denumit în continuare *Sistem*) – totalitatea resurselor şi tehnologiilor informaţionale, mijloacelor tehnice de program, metodologiilor şi personalului, aflate în interconexiune şi destinate păstrării, prelucrării şi utilizării informaţiilor cu caracter criminal în cadrul băncii centrale de date, precum şi evidenţei unice a infracţiunilor;

organe de urmărire penală – organe care, conform legii, au dreptul de a efectua urmărirea penală;

organe de executare a pedepsei penale – Departamentul de executare şi Administraţia Naţională a Penitenciarelor;

infracţiune – faptă (acţiune sau inacţiune) prejudiciabilă, prevăzută de legea penală, săvîrşită cu vinovăţie şi pasibilă de pedeapsă penală;

evidenţă unică – înregistrarea şi evidenţa centralizată a infracţiunilor, la momentul începerii urmăririi penale, şi a persoanelor care au săvîrşit infracţiuni, începînd cu ziua punerii sub învinuire, rectificarea datelor în funcţie de rezultatele urmăririi penale, judecării cauzei şi executării pedepsei privative de libertate sau a altei pedepse;

înregistrare – includerea informaţiei în banca centrală de date, cu atribuirea numărului de ordine fiecărei informaţii;

evidenţă centralizată – evidenţa informaţiei cu caracter criminal în cadrul băncii centrale de date; substituit prin LP245 din15.11.18 MO 462-466 din12.12.18 art. 774

bază de date – totalitatea datelor cu caracter criminal, organizate conform unei anumite structuri conceptuale, cu descrierea caracteristicilor acestor date, ţinîndu-se cont de conexiunea dintre părţile lor componente, care se utilizează la combaterea criminalităţii;

bancă centrală de date – totalitatea informaţiilor parvenite din băncile locale de date şi produselor de program pentru dirijarea bazelor de date, precum şi a masivelor informaţionale manuale cu caracter criminal;

bancă locală de date – totalitatea bazelor de date ale participantului la Sistem şi produselor de program pentru dirijarea lor;

sesizare despre infracţiune – plîngere, denunţ, autodenunţ, raport al lucrătorului organului de urmărire penală despre depistarea nemijlocită a infracţiunii;

alte informaţii despre infracţiuni – informaţii care necesită verificare în scopul constatării elementelor infracţiunii;

informaţie cu caracter criminal – informaţie despre infracţiunile înregistrate şi persoanele care le-au săvîrşit, despre alte categorii de persoane luate la evidenţa centralizată specială în conformitate cu prezenta lege, despre obiectele marcate şi obiectele de anticariat, alte date ce caracterizează infracţiunile şi circumstanţele comiterii lor;

obiecte marcate – mijloace de transport, arme de foc şi arme albe, tehnică de calcul şi de multiplicare, alte obiecte, care pot fi identificate prin numărul respectiv al producătorului;

acte de evidenţă primară – fişe, registre, caziere judiciare, notificări şi alte acte;

formulare-tip ale actelor de evidenţă primară – acte de evidenţă primară aprobate în modul stabilit;

alţi purtători de informaţie – copii de pe actele procedurale;

forme ale rapoartelor statistice – forme ale rapoartelor statistice generalizate şi departamentale privind starea infracţionalităţii, rezultatele descoperirii infracţiunilor, urmăririi penale, examinării judiciare, precum şi privind executarea pedepsei privative de libertate sau altei pedepse;

numărul de infracţiuni a căror urmărire penală a fost terminată – numărul de infracţiuni ale căror dosare penale au fost transmise în instanţele de judecată sau au fost clasate pe temei de nereabilitare;

protecţia informaţiei (datelor) – activitate orientată spre asigurarea securităţii informaţiei (datelor);

securitatea informaţiei (datelor) – protecţia tehnică, de program şi fizică a informaţiei (datelor) de pericole interne şi externe.

Articolul 3. Principiile creării şi funcţionării Sistemului

Sistemul se creează şi funcţionează în baza următoarelor principii:

a) evidenţa unică şi înregistrarea centralizată a infracţiunilor şi a persoanelor care le-au săvîrşit;

b) înregistrarea informaţiei în ordine cronologică;

c) atribuirea fiecărei informaţii a unui număr în ordinea înregistrării ei;

d) utilizarea formularelor-tip ale actelor de evidenţă primară;

e) temeinicia, plenitudinea, veridicitatea şi oportunitatea prezentării informaţiei;

f) accesul sancţionat şi limitat la informaţie;

g) protecţia şi securitatea informaţiei;

h) controlul asupra utilizării informaţiei.

Articolul 4. Funcţiile Sistemului

Sistemul are următoarele funcţii:

1) colectează, acumulează, prelucrează, păstrează şi actualizează informaţia cu caracter criminal;

2) asigură la nivel de stat evidenţa unică:

a) a infracţiunilor şi a persoanelor care le-au săvîrşit (inclusiv locuitorii Republicii Moldova care au săvîrşit infracţiuni pe teritoriul altor state), precum şi a pedepselor aplicate lor;

b) a cauzelor penale şi acţiunilor de urmărire penală;

c) a obiectelor marcate;

d) a persoanelor dispărute fără urmă şi persoanelor date în urmărire;

e) a persoanelor deţinute şi celor aflate în instituţiile penitenciare;

f) a persoanelor eliberate din locurile de detenţie;

g) a altei informaţii cu caracter criminal;

3) asigură cu informaţie operativă şi statistică conducerea ţării, ministerelor şi departamentelor interesate şi organelor de urmărire penală;

4) asigură schimbul de informaţie cu caracter criminal între organele de urmărire penală şi alte autorităţi publice (schimb reciproc de date între sistemele informaţionale departamentale), precum şi cu organele similare din alte ţări;

5) supraveghează respectarea disciplinei de înregistrare şi evidenţă a infracţiunilor şi a persoanelor care le-au săvîrşit, a altei informaţii cu caracter criminal, elaborează şi realizează măsuri de reacţionare oportună la tendinţele şi manifestările negative;

6) asigură din punct de vedere organizatoric, normativ şi metodic activitatea organelor de urmărire penală care exercită nemijlocit funcţiile de evidenţă a informaţiei cu caracter criminal;

7) asigură funcţionarea complexului tehnic de program şi a reţelelor informaţionale utilizate în cadrul Sistemului.

Articolul 5. Participanţii la Sistem

(1) Participanţi la Sistem sînt organele de urmărire penală, instanţele judecătoreşti şi organele de executare a pedepsei privative de libertate.

(2) Participanţii la Sistem:

a) iau parte la crearea, implementarea şi dezvoltarea Sistemului;

b) fac propuneri cu privire la modificarea actelor normative existente care reglementează funcţionarea Sistemului;

c) prezintă şi primesc gratuit informaţia cu caracter criminal conţinută în banca centrală de date şi în băncile locale de date, precum şi rapoartele statistice generalizate;

d) verifică respectarea disciplinei de înregistrare şi evidenţă a informaţiei cu caracter criminal;

e) verifică utilizarea informaţiei cu caracter criminal;

f) asigură protecţia şi securitatea informaţiei cu caracter criminal.

Articolul 6. Finanţarea Sistemului

Finanţarea creării, implementării, funcţionării şi dezvoltării Sistemului se

efectuează din contul mijloacelor prevăzute în bugetul de stat pentru participanţii la Sistem.

Articolul 7. Administrarea băncii centrale de date şi a băncilor locale de date

(1) Administrarea băncii centrale de date, înregistrarea şi evidenţa centralizată a informaţiei cu caracter criminal, precum şi eliberarea rapoartelor statistice generalizate privind starea infracţionalităţii în ţară, se efectuează de către Ministerul Afacerilor Interne, care este deţinătorul băncii centrale de date.

(2) Alte autorităţi publice, care nu sînt participante la Sistem, sînt obligate să prezinte băncii centrale de date informaţia cu caracter criminal în volumul şi în termenele stabilite de către administratorul băncii centrale de date.

(3) Administrarea băncilor locale de date se efectuează de către fiecare participant la Sistem de sine stătător. Acumularea, prelucrarea, păstrarea şi utilizarea informaţiei primare cu caracter criminal în cadrul băncilor locale de date se efectuează de către fiecare participant la Sistem în conformitate cu actele normative departamentale.

Articolul 8. Actualizarea informaţiei

Informaţia cu caracter criminal poate fi rectificată, modificată şi completată în procesul urmăririi penale, examinării judiciare, precum şi pe parcursul executării pedepsei privative de libertate, în baza datelor din diferite acte de evidenţă primară parvenite ulterior.

Articolul 9. Actele de evidenţă primară

(1) Formularele-tip ale actelor de evidenţă primară se întocmesc şi se modifică de către Ministerul Afacerilor Interne şi, după coordonarea lor cu ceilalţi participanţi la Sistem, se aprobă de către Procurorul General.

(2) Schimbarea de sine stătător de către participanţii la Sistem a formei actelor de evidenţă primară se interzice.

(3) Participanţii la Sistem se asigură de sine stătător cu actele de evidenţă primară prevăzute de prezenta lege.

(4) Pentru evidenţa unică a infracţiunilor şi a persoanelor care le-au săvîrşit, se permite utilizarea, în loc de actele de evidenţă primară, a altor purtători de informaţie.

(5) Modalitatea completării şi prezentării actelor de evidenţă primară se stabileşte în conformitate cu instrucţiunile respective, care se elaborează de către Ministerul Afacerilor Interne şi, după coordonarea lor cu ceilalţi participanţi la

Sistem, se aprobă de către Procurorul General.

(6) Actele de evidenţă primară, întocmite în forma stabilită de către participanţii la Sistem, în limita competenţei lor, sînt documente oficiale de evidenţă statistică.

Articolul 10. Modul de elaborare a instrucţiunilor cu privire la evidenţa unică a infracţiunilor şi a persoanelor care le-au săvîrşit

Instrucţiunile cu privire la evidenţa unică a infracţiunilor şi a persoanelor care le-au săvîrşit se elaborează de către Ministerul Afacerilor Interne şi, după coordonarea lor cu ceilalţi participanţi la Sistem, se aprobă de către Procurorul General.

Articolul 11. Organizarea examinării sesizărilor şi a altor informaţii despre infracţiuni

(1) Modul de primire, înregistrare, evidenţă şi examinare a sesizărilor şi a altor informaţii despre infracţiuni se stabileşte de către fiecare participant la Sistem de sine stătător, în conformitate cu legislaţia în vigoare.

(2) Alte informaţii despre infracţiuni se examinează în termenele prevăzute de legislaţia de procedură penală pentru examinarea sesizărilor despre infracţiuni.

(3) Sesizările şi alte informaţii despre infracţiuni se primesc de către participanţii la Sistem pe parcursul zilei de lucru, iar de către organele de urmărire penală a Ministerului Afacerilor Interne – pe parcursul a 24 de ore.

(4) Informaţia despre infracţiuni parvenită se înregistrează în Registrul de evidenţă a sesizărilor cu privire la infracţiuni şi în Registrul de evidenţă a altor informaţii cu privire la infracţiuni.

Capitolul II

EVIDENŢA UNICĂ A INFRACŢIUNILOR ŞI A CAUZELOR PENALE

Articolul 12. Criteriile de evidenţă unică a infracţiunilor şi a cauzelor penale

Înregistrarea centralizată şi evidenţa unică a infracţiunilor şi a cauzelor penale se efectuează după criteriile teritorial şi departamental.

Articolul 13. Actele de evidenţă primară

Pentru evidenţa unică a infracţiunilor, a cauzelor penale şi a materialelor cu privire la infracţiuni, se folosesc următoarele acte de evidenţă primară:

a) fişa infracţiunii constatate;

b) fişa cu privire la derularea cauzei penale, descoperirea infracţiunii şi la alte rezultate ale urmăririi penale;

c) Registrul de evidenţă a infracţiunilor, a cauzelor penale, a persoanelor care au săvîrşit infracţiuni şi a materialelor cu privire la infracţiuni.

Articolul 14. Cazurile în care se completează actele de evidenţă primară a infracţiunilor constatate, a cauzelor penale şi a rezultatelor urmăririi penale

(1) Fişa infracţiunii constatate se completează imediat după începerea urmăririi penale sau examinarea materialelor, precum şi în cazurile:

a) primirii pentru urmărire penală a dosarului penal remis de un alt organ de urmărire penală;

b) reţinerii pentru urmărire penală a dosarului penal pornit în cazul infracţiunii săvîrşite în afara hotarelor Republicii Moldova;

c) reluării urmăririi penale;

d) necesităţii de a rectifica sau de a introduce date care nu au fost reflectate anterior;

e) restituirii din instanţa de judecată a cauzei penale în care a fost pronunţată o sentinţă de achitare pe motiv că fapta nu a fost săvîrşită de inculpat şi reluării urmăririi penale în vederea identificării făptuitorului infracţiunii.

(2) Fişa cu privire la derularea cauzei penale, descoperirea infracţiunii şi la alte rezultate ale urmăririi penale se completează în scopul ţinerii evidenţei centralizate a acţiunilor de urmărire penală, evidenţei derulării cauzelor penale, precum şi necesităţii de a rectifica sau a introduce date care nu au fost reflectate anterior.

Articolul 15. Cazurile în care infracţiunea săvîrşită este luată la evidenţă ca una singură

Infracţiunea va fi luată la evidenţă ca una singură şi va fi completată o singură fişă în cazul:

a) săvîrşirii infracţiunii de un grup de persoane în orice formă de complicitate, prevăzută de Codul penal;

b) săvîrşirii unei fapte prejudiciabile ce atentează asupra diferitor obiecte, dar care, în conformitate cu legislaţia penală, se califică drept o singură infracţiune;

c) infracţiunii în urma săvîrşirii căreia au fost vătămate mai multe persoane;

d) infracţiunii continue ce se caracterizează prin săvîrşirea neîntreruptă a activităţii infracţionale în decursul unui timp nedeterminat;

e) infracţiunii prelungite ce se caracterizează prin două sau mai multe acţiuni infracţionale identice, săvîrşite cu un singur scop, cu o singură intenţie, alcătuind în totalitate o infracţiune;

f) săvîrşirii succesive a unui şir de infracţiuni identice, neînsemnate care, în totalitate, prezintă un pericol social sporit şi sînt prevăzute în Partea specială a Codului penal.

Articolul 16. Cazurile în care infracţiunile se iau la evidenţă ca două şi mai multe

Infracţiunile se iau la evidenţă ca două şi mai multe şi se completează cîteva fişe în cazurile în care:

a) o persoană (un grup de persoane), printr-o singură acţiune (inacţiune), a săvîrşit două sau mai multe infracţiuni prevăzute în diferite articole din Partea specială a Codului penal;

b) o persoană (un grup de persoane), în diferite perioade de timp, a săvîrşit două sau mai multe infracţiuni care nu au fost înregistrate anterior.

Articolul 17. Criteriile de apreciere a rezultatelor activităţii de urmărire penală

(1) Criteriul unic de bază la aprecierea rezultatelor activităţii de urmărire penală la nivel naţional sau la nivel de unitate administrativ-teritorială este numărul de infracţiuni înregistrate centralizat după criteriul teritorial a căror urmărire penală a fost terminată prin adoptarea de către procuror a uneia din următoarele decizii:

a. trimiterea cauzei penale cu rechizitoriu în instanţa de judecată pentru examinare în fond;

b. trimiterea cauzei penale în instanţa de judecată pentru aplicarea măsurilor de constrîngere cu caracter medical;

c. încetarea urmăririi penale sau clasarea cauzei penale;

d. încetarea procesului penal în condiţiile art.495 alin.(1) pct.1) din Codul de procedură penală;

e. suspendarea condiţionată a urmăririi penale;

f. încetarea procesului penal cu liberarea de răspundere penală a minorului;

g. transferul urmăririi penale altui stat.

(2) Ponderea infracţiunilor înregistrate în perioada de gestiune a căror urmărire penală a fost terminată prin adoptarea uneia din deciziile specificate la alin.(1) se calculează raportînd numărul lor, stabilit conform rezultatelor primite de la organele de urmărire penală, la numărul total de infracţiuni înregistrate prima dată în perioada de gestiune în teritoriul respectiv, adică de la 1 ianuarie pînă la data necesară perioadei de gestiune, indiferent de data comiterii infracţiunii.

(3) Alte criterii se stabilesc de către fiecare participant la Sistem de sine stătător, conform criteriilor teritorial şi departamental de evidenţă unică a infracţiunilor şi a cauzelor penale, ţinînd cont de funcţiile executate, prevăzute de legislaţia în vigoare. Criteriile stabilite de sine stătător sînt de uz intern departamental, iar rezultatele estimative obţinute sînt folosite de organele respective pentru necesităţi de serviciu.

Articolul 18. Evidenţa datelor suplimentare cu caracter criminal referitoare la infracţiuni

(1) Înregistrarea şi evidenţa centralizată a altor date cu caracter criminal referitoare la infracţiuni se efectuează în conformitate cu instrucţiunile respective, care se elaborează de către Ministerul Afacerilor Interne şi, după coordonarea lor cu ceilalţi participanţi la Sistem, se aprobă de către Procurorul General.

(2) Datele despre mijloacele de transport furate (răpite), actele de înregistrare, precum şi informaţia despre posesorii acestor mijloace de transport, se introduc în Sistem în baza datelor din Registrul de stat al mijloacelor de transport.

Capitolul III

EVIDENŢA UNICĂ A PERSOANELOR CARE AU SĂVÎRŞIT INFRACŢIUNI ŞI A PEDEPSELOR CE LE-AU FOST APLICATE. EVIDENŢA CENTRALIZATĂ SPECIALĂ A ALTOR CATEGORII DE PERSOANE

Articolul 19. Principiile de evidenţă unică a persoanelor care au săvîrşit infracţiuni şi a pedepselor ce le-au fost aplicate

Înregistrarea centralizată şi evidenţa unică a persoanelor care au săvîrşit infracţiuni şi a pedepselor ce le-au fost aplicate, precum şi evidenţa centralizată specială a altor categorii de persoane, se efectuează după principiile teritorial şi departamental.

Articolul 20. Categoriile de persoane luate la evidenţa centralizată

În cadrul Sistemului se iau la evidenţă centralizată următoarele categorii de persoane:

1) persoanele care au săvîrşit infracţiuni:

a) condamnate pe teritoriul Republicii Moldova şi pe teritoriile altor state;

b) puse sub învinuire;

c) absolvite de răspundere penală: în legătură cu expirarea termenului de prescripţie; ca urmare a unui act de amnistie, dacă prin acesta a fost anulată aplicarea pedepsei pentru infracţiunea săvîrşită; dacă persoana a fost graţiată; în caz de deces; în legătură cu schimbarea situaţiei;

d) aflîndu-se în stare de iresponsabilitate;

e) date în urmărire generală de către organele de urmărire penală ale Republicii Moldova sau ale altor state;

f) reţinute şi arestate pe teritoriul Republicii Moldova cu scopul extrădării;

g) reţinute ca fiind bănuite de săvîrşirea unei infracţiuni;

2) persoanele luate la evidenţă specială în scopul profilaxiei infracţionalităţii.

Articolul 21. Actele de evidenţă primară a persoanelor care au săvîrşit infracţiuni şi a pedepselor

ce le-au fost aplicate

(1) Modul de completare şi prezentare a actelor de evidenţă primară a persoanelor care au săvîrşit infracţiuni, a pedepselor ce le-au fost aplicate, precum şi a altor categorii de persoane luate la evidenţa centralizată specială, este stipulat în instrucţiunile respective, care se elaborează de către Ministerul Afacerilor Interne şi, după coordonarea lor cu ceilalţi participanţi la Sistem, se aprobă de către Procurorul General.

(2) Numărul de stat de identificare al persoanei, datele personale, domiciliul, informaţia privind actele de identitate eliberate persoanei, precum şi datele despre schimbarea numelui, prenumelui sau despre decesul persoanei, se introduc în Sistem în baza datelor din Registrul de stat al populaţiei.

(3) Datele despre mijloacele de transport, documentele de înregistrare, precum şi informaţia despre posesorii acestora, se introduc în Sistem în baza datelor din Registrul de stat al transporturilor.

Capitolul IV

ORGANIZAREA SERVICIULUI INFORMATIV ŞI STATISTIC

Articolul 22. Rapoarte statistice

(1) Elaborarea şi aprobarea formelor rapoartelor statistice departamentale, stabilirea modului şi termenelor de prezentare a acestor rapoarte se efectuează de către participanţii la Sistem de sine stătător, în conformitate cu legislaţia în vigoare.

(2) Elaborarea formelor rapoartelor statistice generalizate privind starea infracţionalităţii în ţară, stabilirea modului şi termenelor de prezentare a acestor rapoarte se efectuează de către Ministerul Afacerilor Interne în comun cu Biroul Naţional de Statistică. Formele menţionate ale rapoartelor, modul şi termenele de prezentare a acestor rapoarte, după coordonarea lor cu ceilalţi participanţi la Sistem, se aprobă de către Procurorul General. Aceste forme ale rapoartelor se prezintă Biroului Naţional de Statistica pentru lucrări statistice şi analitice.

Articolul 23. Activitatea operativ-informativă

(1) Informaţia conţinută în banca centrală de date se eliberează în următoarele cazuri:

a) în scopul efectuării urmăririi penale, precum şi în alte scopuri de serviciu, inclusiv cu caracter operativ;

b) pentru stabilirea antecedentelor penale sau lipsei acestora;

c) pentru identificarea persoanelor şi cadavrelor;

d) la efectuarea de către organele de urmărire penală a măsurilor operative de investigaţii şi de profilaxie;

e) pentru stabilirea locurilor şi termenelor de aflare a persoanelor deţinute în instituţiile penitenciare şi în izolatoarele de detenţie provizorie;

f) la eliberarea cazierului sau certificatului judiciar şi altor certificate;

g) în cazul încorporării în Forţele Armate;

h) la examinarea cererilor privind declararea decesului sau dispariţiei fără urmă a persoanei;

i) la eliberarea de către organele abilitate a actelor de identitate;

k) la indicaţia conducerii Ministerului Afacerilor Interne sau altor participanţi la Sistem.

(2) Modul de efectuare a activităţii operativ-informative se stabileşte de către Ministerul Afacerilor Interne.

Articolul 24. Dreptul la primirea informaţiei

Dreptul la primirea informaţiei din banca centrală de date şi din băncile locale de date se acordă:

a) participanţilor la Sistem, în limita competenţei lor;

b) organelor de urmărire penală şi organelor similare acestora din alte state cu care au fost încheiate acorduri respective;

b1) Serviciului de Informaţii şi Securitate;

c) altor persoane fizice şi juridice, în modul stabilit de legislaţia în vigoare.

Articolul 25. Asigurarea protecţiei şi securităţii informaţiei

(1) Participanţii la Sistem protejează prin măsuri adecvate datele colectate, echipamentele tehnice şi produsele de program utilizate pentru administrarea acestora, asigurînd securitatea datelor conţinute în banca centrală de date şi în băncile locale de date împotriva riscurilor de pierdere, distrugere, precum şi împotriva folosirii neautorizate sau divulgării lor.

(2) Asigurarea protecţiei, securităţii şi integrităţii informaţiei conţinute în banca centrală de date, precum şi a accesului nemijlocit la această informaţie, se efectuează de către administratorul băncii centrale de date, în conformitate cu legislaţia în vigoare.

(3) Asigurarea protecţiei, securităţii şi integrităţii informaţiei conţinute în băncile locale de date, precum şi a accesului la această informaţie, se efectuează de către fiecare participant la Sistem de sine stătător, în conformitate cu legislaţia în vigoare.

Capitolul V

RESPONSABILITATEA

Articolul 26. Responsabilitatea personală

(1) Conducătorii participanţilor la Sistem sînt responsabili pentru caracterul complet al înregistrării şi al evidenţei informaţiei cu caracter criminal în conformitate cu prevederile prezentei legi, pentru veridicitatea şi obiectivitatea evidenţei primare şi a rapoartelor statistice, precum şi pentru acordarea ajutorului practic, metodic şi organizatoric necesar.

(2) Conducătorii participanţilor la Sistem poartă răspundere personală

pentru asigurarea protecţiei, securităţii şi integrităţii informaţiei cu caracter criminal, organizarea şi efectuarea accesului sancţionat la banca centrală de date şi la băncile locale de date în conformitate cu legislaţia în vigoare.

(3) Persoanele vinovate de încălcarea prevederilor prezentei legi poartă răspundere disciplinară, materială, administrativă sau penală în conformitate cu legislaţia în vigoare.

(2^1) Ministerul Afacerilor Interne, cel puţin de două ori pe an, la finele fiecărui semestru, verifică corectitudinea şi veridicitatea informaţiei introduse în banca centrală de date de către subdiviziunea specializată şi prezintă rezultatele Procurorului General, care, după caz, poate dispune procurorilor din subordine sau unei comisii mixte efectuarea unor controale suplimentare.

PARLAMENTUL

LEGE *Nr. 133din 08-07-2011*

privind protecţia datelor cu caracter personal

MODIFICAT LP52 din 12.03.20, MO84/14.03.20 art.88; în vigoare 14.03.20

Capitolul I

DISPOZIŢII GENERALE

Articolul 1. Scopul legii

Scopul prezentei legi este asigurarea protecţiei drepturilor şi libertăţilor fundamentale ale persoanei fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieţii intime, familiale şi private.

Articolul 2. Domeniul de aplicare

(1) Prezenta lege reglementează relaţiile juridice care apar în procesul de prelucrare a datelor cu caracter personal ce fac parte dintr-un sistem de evidenţă sau care sînt destinate să fie incluse într-un asemenea sistem, efectuată în totalitate sau în parte prin mijloace automatizate, precum şi prin alte mijloace decît cele automatizate.

(2) Domeniul de acţiune al prezentei legi se extinde asupra:

a) prelucrării datelor cu caracter personal efectuate în cadrul activităţilor desfăşurate de operatori aflaţi pe teritoriul Republicii Moldova;

b) prelucrării datelor cu caracter personal efectuate în cadrul misiunilor diplomatice şi oficiilor consulare ale Republicii Moldova, precum şi de către alţi operatori aflaţi în afara teritoriului ţării, dar pe teritorii în care se aplică dreptul intern al Republicii Moldova, în temeiul dreptului internaţional public;

c) prelucrării datelor cu caracter personal efectuate de operatori aflaţi în afara teritoriului Republicii Moldova, cu utilizarea mijloacelor aflate pe teritoriul Republicii Moldova, cu excepţia cazului în care aceste mijloace nu sînt utilizate decît în scopul tranzitării pe teritoriul Republicii Moldova a datelor cu caracter personal care fac obiectul prelucrării respective;

d) prelucrării datelor cu caracter personal în cadrul acţiunilor de prevenire şi investigare a infracţiunilor, punerii în executare a sentinţelor de condamnare

şi al altor acţuni din cadrul procedurii penale sau contravenţionale în condiţiile legii.

(3) Prevederile prezentei legi sînt aplicabile persoanei împuternicite de către operator, fără a exclude dreptul de a intenta acţiune în justiţie împotriva operatorului.

(4) Domeniul de acţiune al prezentei legi nu se extinde asupra:

a) prelucrării datelor cu caracter personal efectuate de către operatori exclusiv pentru nevoi personale sau familiale, dacă prin aceasta nu se încalcă drepturile subiecţilor datelor cu caracter personal;

b) prelucrării datelor cu caracter personal atribuite la secret de stat în modul stabilit, cu excepţia celor indicate la alin. (2) lit. d);

c) operaţiunilor de prelucrare şi transmitere transfrontalieră a datelor cu caracter personal ce se referă la făptuitorii sau victimele crimelor de genocid, ale crimelor de război şi ale crimelor împotriva umanităţii.

Articolul 3. Noţiuni principale

Termenii şi expresiile utilizate în prezenta lege au următoarele semnificaţii:

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

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

prelucrarea datelor cu caracter personal – orice operaţiune sau serie de operaţiuni 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, ştergerea sau distrugerea;

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

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

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

terţ – persoană fizică sau persoană juridică de drept public ori de drept privat, alta decît subiectul datelor cu caracter personal, decît operatorul ori persoana împuternicită de către operator şi decît persoana care sub autoritatea directă a operatorului sau a persoanei împuternicite este autorizată să prelucreze date cu caracter personal;

destinatar – orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, căreia îi sînt dezvăluite date cu caracter personal, indiferent dacă este sau nu terţ. Nu sînt considerate destinatari organele din domeniul apărării naţionale, securităţii statului şi ordinii publice, organele de urmărire penală şi instanţele judecătoreşti cărora li se comunică date cu caracter personal în cadrul exercitării competenţelor stabilite de lege;

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

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

Capitolul II

CONDIŢIILE DE BAZĂ PENTRU PRELUCRAREA, STOCAREA ŞI UTILIZAREA DATELOR CU CARACTER PERSONAL

Articolul 4. Caracteristica datelor cu caracter personal

(1) Datele cu caracter personal care fac obiectul prelucrării trebuie să fie:

a) prelucrate în mod corect şi conform prevederilor legii;

b) colectate în scopuri determinate, explicite şi legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau ştiinţifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor prezentei legi, inclusiv privind notificarea către Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, şi cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică şi cea ştiinţifică;

c) adecvate, pertinente şi neexcesive în ceea ce priveşte scopul pentru care sînt colectate şi/sau prelucrate ulterior;

d) exacte şi, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sînt colectate şi ulterior prelucrate se şterg sau se rectifică;

e) stocate într-o formă care să permită identificarea subiecţilor datelor cu caracter personal pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care sînt colectate şi ulterior prelucrate. Stocarea datelor cu caracter personal pe o perioadă mai mare, în scopuri statistice, de cercetare istorică sau ştiinţifică, se va face cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează aceste domenii, şi numai pentru perioada necesară realizării acestor scopuri.

(2) Operatorii au obligaţia să respecte şi să asigure implementarea prevederilor alin. (1).

Articolul 5. Prelucrarea datelor cu caracter personal

(1) Prelucrarea datelor cu caracter personal se efectuează cu consimţământul subiectului datelor cu caracter personal.

(2) Consimţământul privind prelucrarea datelor cu caracter personal poate fi retras în orice moment de către subiectul datelor cu caracter personal. Retragerea consimţământului nu poate avea efect retroactiv.

(3) În cazul subiectului datelor cu caracter personal adult sau minor care este supus măsurii de ocrotire judiciare sub forma tutelei, consimţământul privind prelucrarea datelor cu caracter personal se acordă, în formă scrisă, de către reprezentantul legal, în cazul minorului, sau de către tutore, în cazul adultului.

(3^1) În cazul subiectului datelor cu caracter personal adult care este supus

măsurii de ocrotire judiciare sub forma ocrotirii provizorii sau curatelei, consimţământul privind prelucrarea datelor cu caracter personal se acordă, în formă scrisă, de către persoana ocrotită. Dacă starea acesteia nu-i permite să ia de sine stătător o decizie privind prelucrarea datelor cu caracter personal, ocrotitorul provizoriu sau curatorul va asista persoana ocrotită, prin contrasemnarea acordului, în condiţiile legii.

(4) În cazul decesului subiectului datelor cu caracter personal, consimţământul privind prelucrarea datelor sale se acordă, în formă scrisă, de către succesorii acestuia, dacă un astfel de consimţământ nu a fost dat de subiectul datelor cu caracter personal în timpul vieţii.

(5) Consimţământul subiectului datelor cu caracter personal nu este cerut în cazurile în care prelucrarea este necesară pentru:

a) executarea unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înaintea încheierii contractului, la cererea acestuia;

b) îndeplinirea unei obligaţii care îi revine operatorului conform legii;

c) protejarea vieţii, integrităţii fizice sau a sănătăţii subiectului datelor cu caracter personal;

d) executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terţul căruia îi sînt dezvăluite datele cu caracter personal;

e) realizarea unui interes legitim al operatorului sau al terţului căruia îi sînt dezvăluite datele cu caracter personal, cu condiţia ca acest interes să nu prejudicieze interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal;

f) scopuri statistice, de cercetare istorică sau ştiinţifică, cu condiţia ca datele cu caracter personal să rămînă anonime pe toată durata prelucrării.

g) schimbul de date în condițiile legislației în vigoare cu privire la schimbul de date și interoperabilitate.

Articolul 6. Prelucrarea categoriilor speciale de date cu caracter personal

(1) Prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepţia cazurilor în care:

a) subiectul datelor cu caracter personal şi-a dat consimţământul. În cazul subiectului datelor cu caracter personal în privința căruia a fost instituită mă-

sura de ocrotire judiciară sub forma tutelei, prelucrarea categoriilor speciale de date cu caracter personal se efectuează numai cu obţinerea consimţământului în formă scrisă al tutorelui;

b) prelucrarea este necesară pentru îndeplinirea obligaţiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanţiilor prevăzute de lege şi ţinîndu-se cont de faptul că o eventuală dezvăluire către un terţ a datelor cu caracter personal prelucrate în acest scop poate fi efectuată numai dacă există o obligaţie legală a operatorului în acest sens;

c) prelucrarea este necesară pentru protecţia vieţii, integrităţii fizice sau a sănătăţii subiectului datelor cu caracter personal ori a altei persoane, în cazul în care subiectul datelor cu caracter personal se află în incapacitate fizică sau juridică de a-şi da consimţământul;

d) prelucrarea este efectuată în contextul activităţilor legitime de către asociaţii obşteşti, partide şi alte organizaţii social-politice, de către sindicate, asociaţii de patronat, organizaţii filozofice sau religioase, organizaţii cooperatiste necomerciale, cu condiţia ca prelucrarea să se refere numai la membrii acestora sau la persoanele cu care acestea au contacte permanente în legătură cu scopurile lor şi cu condiţia ca datele să nu fie dezvăluite terţilor fără consimţământul subiecţilor datelor cu caracter personal;

e) prelucrarea se referă la date făcute publice în mod voluntar şi manifest de către subiectul datelor cu caracter personal;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiţie al subiectului datelor cu caracter personal;

g) prelucrarea este necesară în scopul asigurării securităţii statului, al reducerii riscului de declanşare sau în cazul declanşării urgenţelor de sănătate publică, cu condiţia ca aceasta să se efectueze cu respectarea drepturilor subiectului datelor cu caracter personal şi a celorlalte garanţii prevăzute de prezenta lege.

[Art.6 al.(1), lit.g) modificată prin LP52 din 12.03.20, MO84/14.03.20 art.88; în vigoare 14.03.20]

(2) Centrul Naţional pentru Protecţia Datelor cu Caracter Personal poate dispune, din motive întemeiate, interzicerea prelucrării categoriilor speciale de date cu caracter personal, chiar dacă subiectul datelor şi-a dat consimţământul, iar acesta nu a fost retras, cu condiţia ca interdicţia să nu fie înlăturată prin unul din cazurile stabilite la alin. (1) lit. b)–g).

Articolul 7. Prelucrarea datelor cu caracter personal privind starea de sănătate

(1) Prelucrarea datelor cu caracter personal privind starea de sănătate se permite, prin derogare de la prevederile art. 6, în cazul în care:

a) prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente pentru subiectul datelor cu caracter personal sau de gestionare a serviciilor de sănătate care acţionează în interesul subiectului datelor cu caracter personal;

b) prelucrarea este necesară pentru protecţia sănătăţii publice.

(2) Cadrele medicale, instituţiile medico-sanitare şi personalul medical al acestora pot prelucra date cu caracter personal privind starea de sănătate fără autorizaţia Centrului Naţional pentru Protecţia Datelor cu Caracter Personal numai dacă prelucrarea este necesară pentru protejarea vieţii, integrităţii fizice şi a sănătăţii subiecţilor datelor cu caracter personal, precum şi în scopul reducerii riscului de declanşare sau în cazul declanşării urgenţelor de sănătate publică.

[Art.7 al.(2) modificat prin LP52 din 12.03.20, MO84/14.03.20 art.88; în vigoare 14.03.20]

(3) Datele cu caracter personal privind starea de sănătate pot fi prelucrate în scopurile indicate la alin. (1) de către sau sub supravegherea unui cadru medical supus secretului profesional ori de către sau sub supravegherea unei alte persoane supuse unei obligaţii echivalente în ceea ce priveşte secretul profesional.

(4) Datele cu caracter personal privind starea de sănătate se colectează de la subiectul datelor cu caracter personal sau atunci cînd o astfel de prelucrare este necesară în conformitate cu alin. (1).

Articolul 8. Prelucrarea datelor cu caracter personal referitoare la condamnări penale, măsuri procesuale de constrîngere sau sancţiuni contravenţionale

(1) Prelucrarea datelor cu caracter personal referitoare la condamnări penale, măsuri procesuale de constrîngere sau sancţiuni contravenţionale poate fi efectuată numai de către sau sub controlul autorităţilor publice, în limitele competenţelor acordate şi în condiţiile stabilite prin legile ce reglementează aceste domenii.

(2) Registrul informaţiilor criminalistice şi criminologice este ţinut de Ministerul Afacerilor Interne.

Articolul 9. Prelucrarea datelor cu caracter personal avînd funcţie de identificare

Prelucrarea numărului de identificare de stat (IDNP) al persoanei fizice, a amprentelor digitale sau a altor date cu caracter personal avînd o funcţie de identificare de aplicabilitate generală poate fi efectuată în următoarele condiţii:

a) subiectul datelor cu caracter personal şi-a dat consimţămîntul;

b) prelucrarea este prevăzută în mod expres de legislaţie.

Articolul 10. Prelucrarea datelor cu caracter personal şi libertatea de exprimare

Prevederile art. 5, 6 şi 8 nu se aplică în situaţia în care prelucrarea datelor cu caracter personal se face exclusiv în scopuri jurnalistice, artistice sau literare, dacă aceasta se referă la date care au fost făcute publice în mod voluntar şi manifest de către subiectul datelor cu caracter personal sau la date care sînt strîns legate de calitatea de persoană publică a subiectului datelor cu caracter personal sau de caracterul public al faptelor în care acesta este implicat, în condiţiile Legii cu privire la libertatea de exprimare.

Articolul 11. Stocarea şi utilizarea datelor cu caracter personal la încheierea operaţiunilor de prelucrare

(1) Condiţiile şi termenele de stocare a datelor cu caracter personal se stabilesc de legislaţie ţinîndu-se cont de prevederile art. 4 alin. (1) lit. e). La expirarea termenului de stocare, datele cu caracter personal urmează a fi distruse în modul stabilit de lege.

(2) Datele cu caracter personal din registrele de stat, de la data încetării utilizării acestora, pot rămîne la păstrare primind statutul de document de arhivă.

(3) La încheierea operaţiunilor de prelucrare a datelor cu caracter personal, dacă subiectul acestor date nu şi-a dat consimţămîntul pentru o altă destinaţie sau pentru o prelucrare ulterioară, acestea vor fi:

a) distruse;

b) transferate unui alt operator, cu condiţia ca operatorul iniţial să garanteze faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea iniţială;

c) transformate în date anonime şi stocate exclusiv în scopuri statistice, de cercetare istorică sau ştiinţifică.

(4) După decesul subiectului datelor cu caracter personal, datele acestuia se pot utiliza, cu consimţământul succesorilor, în scop de arhivă sau în alte scopuri prevăzute de lege.

Capitolul III

DREPTURILE SUBIECTULUI DATELOR CU CARACTER PERSONAL

Articolul 12. Informarea subiectului datelor cu caracter personal

(1) În cazul în care datele cu caracter personal sînt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată să-i furnizeze următoarele informaţii, exceptînd cazul în care acesta deţine deja informaţiile respective:

1) identitatea operatorului sau, după caz, a persoanei împuternicite de către operator;

2) scopul prelucrării datelor colectate;

3) informaţii suplimentare, precum:

a) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

b) existenţa drepturilor de acces la date, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care acestea pot fi exercitate;

c) dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, precum şi consecinţele posibile ale refuzului de a răspunde.

(2) În cazul în care datele cu caracter personal nu sînt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată ca, în momentul colectării datelor sau, dacă se intenţionează dezvăluirea acestora către terţi, cel mai tîrziu în momentul primei dezvăluiri, să furnizeze subiectului datelor cu caracter personal informaţia privind categoriile de date care urmează a fi colectate sau dezvăluite, precum şi informaţiile indicate la alin. (1), cu excepţia pct. 3) lit. c).

(3) Prevederile alin. (2) nu se aplică în cazul în care:

a) subiectul datelor cu caracter personal deţine informaţiile respective;

b) prelucrarea datelor cu caracter personal se face în scopuri statistice, de cercetare istorică sau ştiinţifică;

c) furnizarea informaţiilor este imposibilă sau implică un efort disproporţio-

nat faţă de interesul legitim care ar putea fi lezat;

d) înregistrarea sau dezvăluirea datelor cu caracter personal este prevăzută în mod expres de legislaţie.

Articolul 13. Dreptul de acces la datele cu caracter personal

(1) Orice subiect al datelor cu caracter personal are dreptul să obţină de la operator, la cerere, fără întîrziere şi în mod gratuit:

a) confirmarea faptului că datele care îl privesc sînt sau nu sînt prelucrate de acesta, de asemenea informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sînt dezvăluite datele;

b) comunicarea, într-o formă inteligibilă şi într-un mod care nu necesită un echipament suplimentar, a datelor cu caracter personal care fac obiectul prelucrării, precum şi a oricărei informaţii disponibile privind originea acestor date;

c) informaţii privind principiile de funcţionare a mecanismului prin care se efectuează prelucrarea automatizată a datelor care vizează subiectul datelor cu caracter personal;

d) informaţii cu privire la consecinţele juridice generate de prelucrarea datelor cu caracter personal pentru subiectul acestor date;

e) informaţii privind modul de exercitare a dreptului de intervenţie asupra datelor cu caracter personal.

(2) În cazul în care datele cu caracter personal privind starea de sănătate sînt prelucrate în scop de cercetare ştiinţifică, dacă nu există riscul de a se aduce atingere drepturilor subiectului datelor cu caracter personal şi dacă datele nu sînt utilizate pentru a lua decizii sau măsuri faţă de o anumită persoană, comunicarea informaţiilor prevăzute la alin. (1) se poate face într-un termen mai mare decît cel stabilit de Legea privind accesul la informaţie, în măsura în care aceasta ar putea afecta cercetarea sau rezultatul acesteia, dar nu mai tîrziu de momentul în care cercetarea este încheiată. Subiectul datelor cu caracter personal trebuie să îşi dea consimţămîntul ca datele privind starea de sănătate să fie prelucrate în scop de cercetare ştiinţifică, precum şi asupra posibilei amînări din acest motiv a comunicării informaţiilor prevăzute la alin. (1).

Articolul 14. Dreptul de intervenţie asupra datelor cu caracter personal

Orice subiect al datelor cu caracter personal are dreptul de a obţine de la operator sau persoana împuternicită de către acesta, la cerere şi în mod gratuit:

a) rectificarea, actualizarea, blocarea sau ştergerea datelor cu caracter personal a căror prelucrare contravine prezentei legi, în special datorită caracterului incomplet sau inexact al datelor;

b) notificarea terţilor cărora le-au fost dezvăluite datele cu caracter personal despre operaţiunile efectuate conform lit. a), exceptînd cazurile cînd această notificare se dovedeşte a fi imposibilă sau presupune un efort disproporţionat faţă de interesul legitim care ar putea fi lezat.

Articolul 15. Excepţii şi restricţii

(1) Prevederile art. 4 alin. (1), art. 12 alin. (1) şi (2), art.13, 14 şi 28 nu se aplică în cazul în care prelucrarea datelor cu caracter personal este efectuată în cadrul acţiunilor prevăzute la art. 2 alin. (2) lit. d) şi la art. 5 alin. (5) lit. g), în scopul apărării naţionale, al securităţii statului şi menţinerii ordinii publice, al protecţiei drepturilor şi libertăţilor subiectului datelor cu caracter personal sau ale altor persoane, dacă prin aplicarea acestora este prejudiciată eficienţa acţiunii sau obiectivul urmărit în exercitarea competenţelor legale ale autorităţii publice.

(2) Prelucrarea datelor cu caracter personal în scopurile stabilite la alin. (1) nu poate depăşi perioada necesară atingerii obiectivului urmărit.

(3) După încetarea situaţiei care justifică aplicarea alin. (1) şi (2) din prezentul articol, operatorii vor lua măsurile necesare pentru a asigura respectarea drepturilor subiecţilor datelor cu caracter personal prevăzute la art. 12–14.

(4) Autorităţile publice ţin evidenţa aplicării excepţiilor stabilite la alin. (1) şi informează Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, în termen de 10 zile, despre datele cu caracter personal prelucrate în condiţiile prezentului articol.

Articolul 16. Dreptul de opoziţie al subiectului datelor cu character personal

(1) Subiectul datelor cu caracter personal are dreptul de a se opune în orice moment, în mod gratuit, din motive întemeiate şi legitime legate de situaţia sa particulară, ca datele cu caracter personal care îl vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care legea stabileşte altfel. Dacă opoziţia este justificată, prelucrarea efectuată de operator nu mai poate viza aceste date.

(2) Subiectul datelor cu caracter personal are dreptul de a se opune în orice moment, în mod gratuit şi fără nici o justificare, ca datele care îl vizează să fie prelucrate pentru prospectare comercială. Operatorul sau persoana împuternicită de către operator este obligată să informeze subiectul despre dreptul de a se opune unei astfel de lucrări înaintea dezvăluirii către terţi a datelor sale cu

caracter personal.

Articolul 17. Dreptul de a nu fi supus unei decizii individuale

(1) Orice persoană are dreptul de a cere anularea, în totalitate sau parţală, a oricărei decizii individuale care produce efecte juridice asupra drepturilor şi libertăţilor sale, fiind întemeiată exclusiv pe prelucrarea automatizată a datelor cu caracter personal destinată să evalueze unele aspecte ale personalităţii sale, precum competenţa profesională, credibilitatea, comportamentul şi altele asemenea.

(2) Persoana poate fi supusă deciziei prevăzute la alin. (1) în cazul în care:

a) decizia este autorizată de o lege care stabileşte măsurile ce garantează apărarea interesului legitim al subiectului datelor cu caracter personal;

b) decizia este luată în cadrul încheierii sau executării unui contract, cu condiţia că cererea de încheiere sau de executare a contractului depusă de subiectul datelor cu caracter personal a fost satisfăcută.

Articolul 18. Accesul la justiţie

Orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal efectuată ilegal sau căreia i-au fost încălcate drepturile şi interesele garantate de prezenta lege are dreptul de a sesiza instanţa de judecată pentru repararea prejudiciilor materiale şi morale.

Capitolul IV

ORGANUL DE CONTROL AL PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

Articolul 19. Organul de control al prelucrărilor de date cu caracter personal

(1) Controlul asupra conformităţi prelucrării datelor cu caracter personal cu cerinţele prezentei legi se efectuează de către Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (în continuare – Centru), care acţionează în condiţii de imparţialitate şi independenţă.

(2) Centrul este persoană juridică, dispune de ştampilă şi de antet cu imaginea Stemei de Stat a Republicii Moldova. Sediul permanent al Centrului se află în municipiul Chişinău.

(3) Regulamentul Centrului, structura şi personalul-limită ale acestuia se aprobă de Parlament.

(4) Centrul se finanţează de la bugetul de stat în limita alocaţiilor bugetare

aprobate prin legea bugetară anuală.

(5) Bugetul Centrului se elaborează, se aprobă şi se administrează conform principiilor, regulilor şi procedurilor prevăzute de Legea finanțelor publice şi responsabilității bugetar-fiscale nr. 181/2014.

Articolul 20. Atribuţiile şi drepturile Centrului

(1) Centrul are următoarele atribuţii:

a) monitorizează respectarea legislaţiei cu privire la protecţia informaţiei şi controlează aplicarea acesteia, în special dreptul la informare, de acces la date, de intervenţie asupra datelor şi de opoziţie;

b) autorizează prelucrările de date cu caracter personal în cazurile prevăzute de lege;

c) emite instrucţiunile necesare pentru a aduce prelucrările de date cu caracter personal în conformitate cu prevederile prezentei legi, fără a atinge sfera de competenţă a altor organe;

d) oferă subiecţilor datelor cu caracter personal informaţii referitoare la drepturile lor;

e) dispune suspendarea sau încetarea prelucrării datelor cu caracter personal efectuate cu încălcarea prevederilor prezentei legi;

f) ţine registrul de evidenţă al operatorilor de date cu caracter personal, ale cărui formă şi conţinut se aprobă de Guvern; registrul este public, cu excepţia informaţiei prevăzute la art. 23 alin. (2) lit. l);

g) emite ordine în domeniul protecţiei datelor cu caracter personal şi formulare tipizate ale notificărilor şi ale registrelor proprii;

h) primeşte şi analizează notificările privind prelucrarea datelor cu caracter personal;

i) efectuează controlul legalităţii prelucrărilor de date cu caracter personal conform unui regulament pe care îl elaborează şi îl aprobă;

j) face propuneri privind perfecţionarea legislaţiei în vigoare în domeniul protecţiei şi prelucrării datelor cu caracter personal;

k) cooperează cu autorităţile publice, cu mijloacele de informare în masă, cu asociaţiile obşteşti şi cu instituţiile similare din străinătate;

l) centralizează şi analizează rapoartele anuale de activitate a autorităţilor publice privind protecţia persoanelor în ceea ce priveşte prelucrarea datelor cu

caracter personal;

m) sesizează organele de drept în cazul existenţei unor indicii privind săvîrşirea infracţiunilor legate de încălcarea drepturilor subiecţilor datelor cu caracter personal;

n) constată contravenţii şi încheie procese-verbale conform Codului contravenţional al Republicii Moldova;

o) informează autorităţile publice despre situaţia din domeniul protecţiei drepturilor subiecţilor datelor cu caracter personal, de asemenea răspunde la demersurile şi interpelările acestora;

p) efectuează controlul îndeplinirii Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţonale de date cu caracter personal, aprobate de Guvern;

q) informează periodic instituţiile şi societatea despre activitatea sa, despre problemele şi preocupările prioritare în domeniul protecţiei drepturilor persoanei;

r) acordă asistenţă şi execută cereri de asistenţă privind punerea în practică a Convenţiei pentru protecţia persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal;

s) îndeplineşte alte atribuţii prevăzute de lege.

(2) Centrul are următoarele drepturi:

a) solicită şi primeşte gratuit de la persoane fizice sau persoane juridice de drept public şi de drept privat informaţiile necesare pentru exercitarea atribuţiilor sale;

b) obţine de la operatori suportul şi informaţiile necesare executării atribuţiilor sale;

c) atrage specialişti şi experţi din domenii care necesită cunoştinţe speciale pentru participarea la procesul de verificare prealabilă şi de control al legalităţii prelucrării datelor cu caracter personal şi încheie cu ei acorduri de confidenţialitate;

d) cere de la operatori rectificarea, blocarea sau distrugerea datelor cu caracter personal neveridice sau obţinute ilicit.

(3) Operatorii, indiferent de forma lor juridică de organizare, prezintă Centrului materialele şi documentele solicitate cu privire la protecţia datelor cu caracter personal în termen de 15 zile, dacă în solicitare nu se prevede un alt

termen.

Articolul 21. Organizarea activităţii Centrului

(1) În cadrul activităţii sale, Centrul asigură confidenţialitatea datelor cu caracter personal care i-au devenit cunoscute.

(2) În scopul colectării informaţiilor necesare îndeplinirii atribuţiilor de control, personalul Centrului are dreptul de acces în încăperile şi pe teritoriul în care sînt amplasate sisteme de evidenţă a datelor cu caracter personal, la datele cu caracter personal prelucrate de operatori şi/sau persoanele împuternicite de către aceştia, la echipamentul de prelucrare, programe şi aplicaţii, precum şi la orice document sau înregistrare referitoare la prelucrarea de date cu caracter personal, în condiţiile legii.

(3) Anual, pînă la data de 15 martie, Centrul prezintă Parlamentului, Preşedintelui Republicii Moldova şi Guvernului raportul de activitate pe anul precedent, care se publică gratuit în Monitorul Oficial al Republicii Moldova şi pe pagina web a Centrului.

Articolul 22. Conducerea Centrului

(1) Centrul este condus de un director, numit în funcţie de Parlament la propunerea Preşedintelui Parlamentului, a unei fracţiuni parlamentare sau a unui grup de cel puţin 15 deputaţi, cu votul majorităţii deputaţilor aleşi, pentru un mandat de 5 ani. Persoana numită poate ocupa funcţia de director nu mai mult de două mandate consecutive.

(2) Directorul efectuează conducerea generală a Centrului, angajează şi eliberează personalul Centrului în condiţiile Legii cu privire la funcţia publică şi statutul funcţionarului public, stabileşte obligaţiile de serviciu ale acestuia, organizează pregătirea rapoartelor anuale şi le prezintă în plenul Parlamentului, reprezintă instituţia în ţară şi peste hotare.

(3) În exercitarea atribuţiilor sale, directorul este asistat de un adjunct, numit în funcţie de Parlament la propunerea directorului Centrului, cu votul majorităţii deputaţilor aleşi, pentru un mandat de 5 ani. În absenţa directorului Centrului, directorul adjunct îndeplineşte temporar atribuţiile acestuia.

(4) În funcţia de director sau director adjunct al Centrului poate fi numită orice persoană care deţine cetăţenia Republicii Moldova, are studii superioare juridice şi experienţă profesională de cel puţin 5 ani în domeniul apărării drepturilor şi a libertăţilor omului. Nu pot fi numite în funcţiile de director sau director adjunct al Centrului persoanele în privinţa cărora există interdicţia de a ocupa funcţii publice sau de demnitate publică, ce derivă din actele de constatare ale

Autorității Naționale de Integritate.

(5) Funcţia de director şi cea de director adjunct al Centrului sînt funcţii de demnitate publică, şi se supun prevederilor legislației cu privire la statutul persoanelor care exercită funcţii de demnitate publică. Salarizarea acestor funcţii se face în conformitate cu legislația privind sistemul de salarizare în sectorul bugetar.

(6) Pe perioada exercitării mandatului, directorul şi directorul adjunct al Centrului nu pot face parte din partide sau alte organizaţii social-politice, nu pot desfăşura alte activităţi publice sau private, cu excepţia activităţii didactico-ştiinţifice, nu au dreptul să deţină, direct sau indirect, valori mobiliare la societăţi comerciale sau întreprinderi al căror obiect de activitate se află în competenţa Centrului.

(7) Exercitarea mandatelor de director şi director adjunct încetează la expirarea termenului acestora, exceptînd cazurile de încetare a exercitării atribuţiilor înainte de termen. În cazul în care termenul de exercitare a mandatelor a expirat, directorul şi directorul adjunct al Centrului continuă să se afle în exerciţiul funcţiunii pînă la preluarea acestor funcţii de către succesorii lor.

(8) Mandatele de director şi director adjunct al Centrului încetează înainte de termen în caz de:

a) demisie;

b) incompatibilitate cu alte funcţii publice sau private, stabilită prin actul de constatare rămas definitiv;

c) revocare din funcţie;

d) imposibilitate de a exercita mandatul din motive de sănătate, constatate prin examen medical;

e) deces.

(9) Propunerea de revocare din funcţie a directorului Centrului poate fi înaintată de Preşedintele Parlamentului, de o fracţiune parlamentară sau de un grup de cel puţin 15 deputaţi în următoarele cazuri:

a) încălcare gravă a obligaţiilor funcţionale prevăzute de legislaţie;

b) hotărîre de condamnare rămasă definitivă în cazul săvîrşirii unei infracţiuni;

c) stabilire, prin actul de constatare rămas definitiv, a emiterii/adoptării de către acesta a unui act administrativ, încheierii directe sau prin intermediul unei

persoane terțe a unui act juridic, luării sau participării la luarea unei decizii fără soluționarea conflictului de interese real în conformitate cu prevederile legislației privind reglementarea conflictului de interese;

d) nedepunere a declarației de avere şi interese personale sau refuz de a o depune, în condițiile art. 27 alin. (8) din Legea nr. 132 din 17 iunie 2016 cu privire la Autoritatea Națională de Integritate;

e) dispunere de către instanța de judecată, prin hotărîre irevocabilă, a confiscării averii nejustificate.

(10) Propunerea de revocare din funcție a directorului adjunct al Centrului poate fi înaintată de directorul Centrului, de o fracțiune parlamentară sau de un grup de cel puțin 15 deputați în cazurile prevăzute la alin. (9). Hotărîrea de revocare se adoptă cu votul majorității deputaților aleşi.

Capitolul V

CONTROLUL PROTECȚIEI DATELOR

CU CARACTER PERSONAL

Articolul 23. Notificarea Centrului privind prelucrarea datelor cu caracter personal

(1) Operatorii sînt obligaţi să notifice Centrul, personal sau prin persoanele împuternicite de către ei, înainte de a prelucra date cu caracter personal destinate să servească unui scop. Prelucrarea altor categorii de date cu caracter personal decît cele notificate anterior se va efectua cu condiţia unei noi notificări.

(1^1) Modul de solicitare, acordare, suspendare şi retragere a actelor permisive prevăzute de prezenta lege pentru agenții economici se stabileşte de Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător în partea în care nu este reglementat de prezenta lege.

(2) Notificarea trebuie să conţină următoarele informaţii:

a) numele sau denumirea şi domiciliul ori sediul în Republica Moldova ale operatorului şi ale persoanei împuternicite de către acesta, dacă este cazul;

b) scopul prelucrării;

c) descrierea subiecţilor datelor cu caracter personal, descrierea datelor ce vor fi prelucrate, precum şi a surselor de provenienţă a acestor date;

d) existenţa consimţămîntului subiectului datelor cu caracter personal privind prelucrarea acestora;

e) modul în care subiecţii datelor cu caracter personal sînt informaţi asupra drepturilor lor; data estimată pentru încheierea operaţiunilor de prelucrare, precum şi destinaţia ulterioară a datelor cu caracter personal;

f) destinatarii cărora se intenţionează să li se dezvăluie datele cu caracter personal;

g) garanţiile privind transmiterea datelor cu caracter personal către terţi;

h) propuneri privind transferurile transfrontaliere ale datelor cu caracter personal care se intenţionează să fie făcute;

i) persoanele responsabile pentru prelucrarea datelor cu caracter personal;

j) specificarea sistemelor de evidenţă a datelor cu caracter personal care au legătură cu prelucrarea, precum şi a eventualelor legături cu alte prelucrări de date sau cu alte sisteme de evidenţă a datelor cu caracter personal, indiferent dacă se efectuează sau nu, respectiv dacă sînt situate sau nu pe teritoriul Republicii Moldova;

k) motivele care justifică aplicarea prevederilor art.10 şi art.12 alin. (3), în situaţia în care prelucrarea datelor se face exclusiv în scopuri jurnalistice, artistice sau literare ori în scopuri statistice, de cercetare istorică sau ştiinţifică;

l) descrierea generală a măsurilor luate pentru asigurarea securităţii prelucrării datelor cu caracter personal conform prevederilor art. 30.

(3) În cazul în care datele cu caracter personal care sînt prelucrate urmează să fie transferate către alte state, notificarea va cuprinde suplimentar:

a) categoriile de date care vor face obiectul transferului;

b) statul de destinaţie pentru fiecare categorie de date.

(4) Autorităţile publice care efectuează prelucrări de date cu caracter personal în legătură cu activităţile indicate la art. 2 alin. (2) lit. d), pentru exercitarea atribuţiilor legale ce ţin de sfera lor de competenţă sau pentru îndeplinirea obligaţiilor asumate prin acorduri internaţionale la care Republica Moldova este parte, sînt obligate să depună o declaraţie de informare care va conţine:

a) denumirea şi sediul operatorului sau, după caz, a persoanei împuternicite de către acesta;

b) scopul şi temeiul legal al prelucrării;

c) categoriile de date cu caracter personal supuse prelucrării.

(5) Notificarea nu este necesară în cazul în care prelucrarea are ca scop ţi-

nerea unui registru destinat informării publicului larg şi deschis spre consultare publicului sau oricărei persoane care probează un interes legitim, cu condiţia ca prelucrarea să se limiteze la datele necesare ţinerii registrului menţionat.

(6) Centrul poate stabili şi alte situaţii în care notificarea nu este necesară sau situaţii în care notificarea se poate efectua într-o formă simplificată, numai dacă:

1) prelucrarea, ţinînd cont de natura datelor cu caracter personal, nu afectează drepturile subiecţilor datelor cu caracter personal, cu condiţia precizării:

a) scopului în care se face o asemenea prelucrare;

b) datelor care vor fi prelucrate;

c) categoriilor de subiecţi ai datelor cu caracter personal;

d) destinatarilor cărora datele cu caracter personal le vor fi transmise;

e) perioadei de stocare a datelor cu caracter personal;

2) prelucrarea se efectuează în condiţiile art. 6 alin. (1) lit. d).

(7) În cazul prelucrărilor datelor cu caracter personal nesupuse notificării, operatorul sau persoana împuternicită de către acesta prezintă, la cerere, subiectului datelor cu caracter personal informaţiile prevăzute la alin. (2) lit. a)–k), cu excepţia situaţiei prevăzute la alin. (5).

(8) La notificarea primară, fiecare operator primeşte un număr de înregistrare care se indică pe toate actele prin care datele cu caracter personal sînt colectate, stocate sau transmise.

Articolul 24. Verificarea prealabilă

(1) Dacă pe baza notificării Centrul constată că prelucrarea se încadrează în una din categoriile menţionate la alin. (2), va dispune obligatoriu efectuarea unei verificări prealabile şi va anunţa operatorul sau persoana împuternicită de către acesta în termen de 5 zile de la data depunerii notificării.

(2) Sînt supuse verificării prealabile categoriile de operaţiuni de prelucrare a datelor cu caracter personal care fac obiectul transmiterii transfrontaliere, precum şi categoriile de operaţiuni de prelucrare a datelor cu caracter personal care prezintă riscuri speciale pentru drepturile şi libertăţile persoanelor, după cum urmează:

a) operaţiunile de prelucrare a categoriilor speciale de date cu caracter personal, de asemenea a datelor genetice, biometrice şi a celor care permit localizarea geografică a persoanelor, inclusiv în scop de cercetare ştiinţifică;

b) operaţiunile de prelucrare a datelor cu caracter personal prin mijloace electronice avînd ca scop evaluarea unor aspecte ale personalităţii, precum competenţa profesională, credibilitatea, comportamentul şi altele asemenea;

c) operaţiunile de prelucrare a datelor cu caracter personal prin mijloace electronice în cadrul unor sisteme de evidenţă avînd ca scop adoptarea unor decizii automate individuale în legătură cu analizarea solvabilităţii, a situaţiei economico-financiare, a faptelor susceptibile de a atrage răspunderea disciplinară, contravenţională sau penală a persoanelor fizice, efectuate de către persoanele de drept privat;

d) operaţiunile de prelucrare a datelor cu caracter personal ale minorilor în cadrul activităţilor de prospectare comercială;

e) operaţiunile de prelucrare a datelor cu caracter personal menţionate la lit. a) şi a datelor cu caracter personal ale minorilor, colectate prin intermediul internetului sau mesageriei electronice.

(3) Verificarea prealabilă se efectuează pe baza informaţiilor prezentate în notificare de operator sau persoana împuternicită de către acesta. Centrul poate solicita şi alte informaţii privind originea datelor cu caracter personal, tehnologia de prelucrare automatizată utilizată, măsurile de securitate a prelucrării datelor cu caracter personal.

(4) Durata verificării prealabile nu poate depăşi 45 de zile. În caz de necesitate, ţinînd cont de complexitatea operaţiunilor de prelucrare a datelor cu caracter personal, Centrul poate prelungi termenul de verificare prealabilă cu încă 45 de zile, fapt despre care este informat operatorul sau persoana împuternicită de către acesta.

Articolul 25. Autorizarea operaţiunilor de prelucrare a datelor cu caracter personal

(1) În termen de 7 zile de la data finalizării verificării prealabile, Centrul emite decizia privind autorizarea sau refuzul autorizării operaţiunilor prevăzute la art. 24 alin. (2).

(2) Conţinutul şi forma autorizaţiei se aprobă de Centru. Prelucrarea datelor cu caracter personal fără autorizaţie sau în afara limitelor prevăzute de aceasta este interzisă.

(3) Decizia privind refuzul de a autoriza prelucrarea datelor cu caracter personal trebuie să conţină motivele ce justifică refuzul şi, după caz, modalitatea de înlăturare a circumstanţelor ce împiedică prelucrarea datelor respective. Decizia privind refuzul de a autoriza prelucrarea datelor cu caracter personal poate fi

contestată în instanţa de contencios administrativ.

(4) Refuzul de a autoriza prelucrarea datelor cu caracter personal nu exclude posibilitatea operatorului de a notifica în mod repetat Centrul după înlăturarea circumstanţelor care au împiedicat prelucrarea datelor respective.

Articolul 26. Controlul legalităţii prelucrării datelor cu caracter personal

(1) Controlul legalităţii prelucrării datelor cu caracter personal (în continuare – *control*) are drept scop verificarea corespunderii cu cerinţele şi a îndeplinirii condiţiilor prevăzute de prezenta lege de către operator sau persoana împuternicită de către acesta.

(2) Controlul este efectuat de către Centru în baza unui plan anual aprobat, care se publică pe pagina web a acestuia.

(3) Despre intenţia efectuării controlului, Centrul informează operatorul sau persoana împuternicită de către acesta cu 5 zile înainte de începerea acestuia, cu excepţia cazurilor prevăzute la art. 27 alin. (2) şi (4).

(4) În cazul în care, ca urmare a controlului efectuat, sînt constatate încălcări, Centrul emite decizia de suspendare a operaţiunilor de prelucrare a datelor cu caracter personal, care va conţine instrucţiuni pentru aducerea prelucrării datelor cu caracter personal în conformitate cu prevederile prezentei legi.

(5) Efectuarea operaţiunilor de prelucrare a datelor cu caracter personal se suspendă pînă la înlăturarea circumstanţelor care au servit drept temei pentru emiterea deciziei. Operatorul sau persoana împuternicită de către acesta este obligată să înlăture respectivele circumstanţe în termen de 30 de zile de la emiterea deciziei de suspendare.

(6) În cazul în care operatorul sau persoana împuternicită de către acesta nu a înlăturat circumstanţele care au servit drept temei pentru suspendare în termenul stabilit la alin. (5), Centrul emite decizia de încetare a operaţiunilor de prelucrare a datelor cu caracter personal, cu sau fără dispunerea blocării ori distrugerii datelor cu caracter personal neveridice sau obţinute ilicit.

(7) Decizia de suspendare sau de încetare a operaţiunilor de prelucrare a datelor cu caracter personal poate fi contestată în instanţa de contencios administrativ.

Articolul 27. Procedura primirii şi soluţonării plîngerilor de către Centru

(1) Subiectul datelor cu caracter personal care consideră că prelucrarea datelor sale nu este conformă cu cerinţele prezentei legi poate înainta Centrului o plîngere în termen de 30 de zile din momentul depistării încălcării.

(2) În procesul soluţionării plîngerii, Centrul poate audia subiectul datelor cu caracter personal, operatorul şi, dacă este cazul, persoana împuternicită de către operator şi martorii, de asemenea poate dispune efectuarea unui control inopinat.

(3) În urma examinării plîngerii, Centrul emite o decizie motivată care prevede fie lipsa încălcării prevederilor legislaţiei, fie suspendarea operaţiunilor de prelucrare a datelor cu caracter personal, fie rectificarea, blocarea sau distrugerea datelor neveridice ori obţinute ilicit. Decizia este comunicată părţilor interesate în termen de 30 de zile de la data primirii plîngerii.

(4) Prevederile alin. (2) şi (3) se aplică în mod corespunzător şi în situaţia în care Centrul se autosesizează cu privire la comiterea unei încălcări a drepturilor subiecţilor datelor cu caracter personal, recunoscute de prezenta lege.

(5) Operatorul, persoana împuternicită de către acesta sau subiectul datelor cu caracter personal pot contesta decizia Centrului în instanţa de contencios administrativ.

Articolul 28. Registrul de evidenţă al operatorilor de date cu caracter personal

(1) În scopul evidenţei prelucrărilor de date cu caracter personal, Centrul instituie şi administrează un registru de evidenţă al operatorilor de date cu caracter personal care trebuie să cuprindă informaţiile stabilite la art. 23 alin. (2). Orice modificare a informaţiilor respective va fi comunicată Centrului în termen de 5 zile, care va efectua menţiunile corespunzătoare în registrul de evidenţă al operatorilor de date cu caracter personal.

(2) Registrul de evidenţă al operatorilor de date cu caracter personal este deschis spre consultare publicului, cu excepţia compartimentului care conţine informaţii privind măsurile de securitate şi de asigurare a confidenţialităţii. Modalitatea de consultare se stabileşte de Centru.

(3) Înregistrarea operatorilor, precum şi a modificărilor informaţiilor înscrise în registrul de evidenţă al operatorilor de date cu caracter personal, se efectuează gratuit.

Capitolul VI

CONFIDENŢIALITATEA ŞI SECURITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Articolul 29. Confidenţialitatea datelor cu caracter personal

(1) Operatorii şi terţii care au acces la datele cu caracter personal sînt obligaţi să asigure confidenţialitatea acestor date, cu excepţia cazurilor:

a) prelucrarea se referă la date făcute publice în mod voluntar şi manifest de către subiectul datelor cu caracter personal;

b) datele cu caracter personal au fost depersonalizate.

(2) Orice persoană care acţionează în numele, pe seama sau în alt mod sub autoritatea operatorului poate prelucra date cu caracter personal doar pe baza instrucţiunilor operatorului, cu excepţia cazului în care acţionează în temeiul unei obligaţii prevăzute de lege.

(3) Conducerea Centrului şi personalul acestuia sînt obligaţi să garanteze nedivulgarea secretului profesional în ceea ce priveşte informaţiile confidenţiale la care au acces, inclusiv după încetarea activităţii lor.

Articolul 30. Securitatea prelucrării datelor cu caracter personal

(1) La prelucrarea datelor cu caracter personal, operatorul este obligat să ia măsurile organizatorice şi tehnice necesare pentru protecţia datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspîndirii, precum şi împotriva altor acţiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce priveşte riscurile prezentate de prelucrare şi caracterul datelor prelucrate.

(2) În cazul în care prelucrarea datelor cu caracter personal este efectuată pe seama şi în numele operatorului, acesta va împuternici o persoană care va asigura respectarea garanţiilor referitoare la măsurile adecvate de securitate tehnică şi de organizare privind prelucrarea ce urmează să fie efectuată.

(3) Prelucrarea datelor cu caracter personal prin persoana împuternicită de către operator trebuie reglementată printr-un contract sau un alt act juridic care să asigure în special faptul că:

a) persoana împuternicită acţionează numai pe baza instrucţiunilor operatorului;

b) obligaţiile prevăzute la alin. (1) îi revin şi persoanei împuternicite.

(4) Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal se stabilesc de Guvern.

Articolul 31. Depersonalizarea datelor cu caracter personal

(1) În scopuri statistice, de cercetare istorică, ştiinţifică, sociologică, med-

icală, de documentare juridică, operatorul depersonalizează datele cu caracter personal prin retragerea din ele a părţii care permite identificarea persoanei fizice, transformîndu-le în date anonime, care nu pot fi asociate cu o persoană identificată sau identificabilă.

(2) În cazul depersonalizării, regimul de confidenţialitate stabilit pentru datele respective se anulează.

Capitolul VII

TRANSMITEREA TRANSFRONTALIERĂ A DATELOR CU CARACTER PERSONAL

Articolul 32. Transmiterea transfrontalieră a datelor cu caracter personal

(1) Prezentul articol se aplică în cazul transmiterii către un alt stat, pe orice suport sau mijloc, a datelor cu caracter personal care constituie obiectul prelucrărilor sau care sînt colectate în scopul de a fi supuse prelucrării.

(2) Datele cu caracter personal destinate transmiterii către un alt stat sînt protejate în conformitate cu prezenta lege.

(3) Transmiterea transfrontalieră a datelor cu caracter personal care fac obiectul unei prelucrări sau care urmează să fie prelucrate după transmitere poate avea loc doar cu autorizarea Centrului, în modul stabilit de lege, şi doar în cazul în care statul de destinaţie asigură un nivel adecvat de protecţie a drepturilor subiecţilor datelor cu caracter personal şi a datelor destinate transmiterii.

(4) Nivelul de protecţie se stabileşte de Centru ţinîndu-se cont de condiţiile în care se realizează transmiterea datelor cu caracter personal, în special de natura acestora, de scopul şi durata prelucrării sau prelucrărilor propuse, de statul de destinaţie, de legislaţia acestuia, precum şi de normele profesionale şi măsurile de securitate respectate în statul de destinaţie.

(5) În cazul în care constată că nivelul de protecţie oferit de statul de destinaţie este nesatisfăcător, Centrul va dispune interzicerea transmiterii datelor.

(6) Centrul poate autoriza, în modul stabilit de lege, transferul de date cu caracter personal către un stat a cărui legislaţie nu prevede un nivel de protecţie cel puţin egal cu cel oferit de legislaţia Republicii Moldova dacă operatorul oferă garanţii suficiente cu privire la protecţia şi exercitarea drepturilor subiecţilor datelor cu caracter personal, care sînt stabilite prin contracte încheiate între operatori şi persoanele fizice sau juridice prin dispoziţia cărora se efectuează transferul.

(7) Prevederile alin. (3)–(6) nu se aplică în cazul în care transferul datelor cu caracter personal se face în baza prevederilor unei legi speciale sau ale unui tratat internaţional ratificat de Republica Moldova, în special dacă transferul se face în scopul prevenirii sau investigării infracţiunilor. Legea specială sau tratatul internaţional trebuie să conţină garanţii privind protecţia drepturilor subiectului datelor cu caracter personal.

(8) Prevederile alin. (1)–(6) nu se aplică în cazul în care prelucrarea datelor cu caracter personal se face exclusiv în scopuri jurnalistice, artistice sau literare, dacă aceste date au fost făcute publice în mod voluntar şi manifest de către subiectul datelor cu caracter personal sau sînt strîns legate de calitatea de persoană publică a acestuia ori de caracterul public al faptelor în care acesta este implicat.

(9) Transmiterea datelor cu caracter personal către statele care nu asigură un nivel adecvat de protecţie poate avea loc numai:

a) cu consimţămîntul subiectului datelor cu caracter personal;

b) în cazul necesităţii de a încheia ori executa un acord sau contract între subiectul datelor cu caracter personal şi operator ori între operator şi o persoană terţă în interesul subiectului datelor cu caracter personal;

c) dacă aceasta este necesară pentru a proteja viaţa, integritatea fizică sau sănătatea subiectului datelor cu caracter personal;

d) dacă aceasta se efectuează dintr-un registru destinat informării publicului larg şi deschis spre consultare publicului sau oricărei persoane care demonstrează un interes legitim, în măsura în care se întrunesc condiţiile prevăzute de lege pentru consultare în cazurile particulare;

e) cînd aceasta este necesară pentru satisfacerea unui interes public major, precum apărarea naţională, securitatea statului sau ordinea publică, pentru buna desfăşurare a procesului penal ori pentru constatarea, exercitarea sau apărarea unui drept în justiţie, cu condiţia ca datele cu caracter personal să fie prelucrate în legătură cu acest scop şi numai pentru perioada necesară realizării acestui scop.

Capitolul VIII

RĂSPUNDEREA

Articolul 33. Răspunderea pentru încălcarea prezentei legi

Pentru încălcarea prezentei legi, persoanele vinovate răspund în conformitate cu legislaţia civilă, contravenţională sau penală.

GUVERNUL

HOTĂRÎRE Nr. 1123 din 14-12-2010

privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal

Publicat : 24-12-2010 în Monitorul Oficial Nr. 254-256 art. 1282

I. DISPOZIŢII GENERALE

1. Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (în continuare – Cerinţe) au drept scop stabilirea regulilor minime de implementare de către deţinătorii de date cu caracter personal a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale de date cu caracter personal şi/sau registrelor ţinute manual, în conformitate cu prevederile Legii nr.17-XVI din 15 februarie 2007 cu privire la protecţia datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2007, nr.107-111, art.468) şi ale Legii nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314).

2. Prezentele Cerinţe creează cadrul necesar aplicării Convenţiei pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiate la Strasbourg la 28 ianuarie 1981, publicate în European Treaty Series, nr. 108, ratificate de Republica Moldova prin Hotărîrea Parlamentului nr. 483-XIV din 2 iulie 1999.

3. În sensul prezentelor Cerinţe, se definesc următoarele noţiuni:

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

control de securitate – acţiuni întreprinse de către deţinătorii de date cu caracter personal sau Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (în continuare – Centrul), în vederea verificării şi/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul

sistemelor informaţionale şi/sau registrelor ţinute manual, în conformitate cu prezentele Cerinţe;

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

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

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

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

nivel de protecţie – nivel de securitate proporţional riscului pe care îl comportă prelucrarea faţă de datele cu caracter personal respective, precum şi faţă de drepturile şi libertăţile persoanelor, stabilit conform Cerinţelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri (N - 1 sau N - 2);

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

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

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

protecţia informaţiei contra acţiunilor neintenţionate – ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau

alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;

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

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

tehnologie informaţională ((TI) eng. informational technology) – totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

utilizator – persoana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;

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

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

stocare – păstrarea pe orice fel de suport a datelor cu caracter personal.

II. CERINŢE GENERALE

4. Măsurile de protecţie a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a sistemului informaţional de date cu caracter personal şi vor fi efectuate neîntrerupt de către toţi deţinătorii de date cu caracter personal.

5. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal.

6. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale de date cu caracter personal se înfăptuiesc ţinîndu-se cont de necesitatea asigurării confidenţialităţii acestor măsuri.

7. Înfăptuirea oricăror măsuri şi lucrări cu folosirea resurselor informaţionale ale deţinătorului de date cu caracter personal este interzisă în cazurile în care nu sînt adoptate şi implementate măsuri corespunzătoare de protecţie a datelor cu caracter personal.

8. Sînt supuse protecţiei toate resursele informaţionale ale deţinătorilor de date cu caracter personal, care conţin date cu caracter personal, inclusiv:

suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;

sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei.

9. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată în scopul:

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

preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;

respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;

asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;

păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.

10. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:

preîntîmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;

excluderea accesului neautorizat la datele cu caracter personal prelucrate;

preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

preîntîmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor angajaţi ai deţinătorului de date cu caracter personal, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program.

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

12. Preîntîmpinarea accesului neautorizat la informaţiile care conţin date cu caracter personal şi circulă sau se păstrează în mijloace tehnice este asigurată prin metoda folosirii mijloacelor speciale tehnice şi de program, cifrării acestor informaţii, inclusiv prin măsurile organizaţionale şi de regim.

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

14. Ordinea de acces la informaţia care conţine date cu caracter personal, prelucrată în cadrul sistemelor informaţionale, se stabileşte de către deţinătorul de date cu caracter personal, în conformitate cu prevederile legislaţiei.

III. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

15. Fiecare deţinător de date cu caracter personal, reieşind din specificul activităţii, elaborează şi organizează implementarea prevederilor documentului care stabileşte politica de securitate a datelor cu caracter personal, inclusiv procedurile şi măsurile legate de realizarea acestei politici, cu aplicarea soluţiilor practice cu un nivel de detalizare şi complexitate proporţional, în partea ce ţine de identificarea şi autentificarea utilizatorilor; de reacţionare la incidentele de securitate; de protecţie a TI şi comunicaţiilor; de asigurare a integrităţii informaţiei care conţine date cu caracter personal şi TI; de administrare a accesului; de audit şi asigurare a evidenţei, luînd în considerare:

1) categoria datelor cu caracter personal prelucrate şi a operaţiunilor de prelucrare efectuate asupra lor (conform anexelor nr.1 şi nr.2 la prezentele Cerinţe);

2) dimensiunea deţinătorului de date cu caracter personal, în funcţie de numărul angajaţilor, numărul subdiviziunilor administrative, amplasarea geografică a subdiviziunilor sau filialelor etc., inclusiv numărul persoanelor care pot accesa datele cu caracter personal;

3) formele de ţinere a registrelor în care sînt prelucrate date cu caracter personal (manuală, electronică sau mixtă);

4) complexitatea sistemelor informaţionale de date cu caracter personal şi programelor de aplicaţii implicate în procesul de prelucrare a datelor;

5) riscurile la care este expus deţinătorul de date cu caracter personal sau persoanele ale căror date cu caracter personal sînt prelucrate, starea de dezvoltare tehnologică în acest domeniu şi costul măsurilor de implementare.

16. Politica de securitate a datelor cu caracter personal se revizuieşte cel puţin o dată în an ca rezultat al modificărilor sau reevaluării componentelor acesteia şi aprobată la cel mai înalt nivel al ierarhiei persoanelor responsabile ale deţinătorului de date cu caracter personal.

Pentru ca politica de securitate a datelor cu caracter personal să fie cunoscută tuturor, acest document este adus la cunoştinţă utilizatorilor şi altor angajaţi ai deţinătorului de date cu caracter personal, în limitele competenţelor funcţionale şi nivelului de acces acordat.

17. Deţinătorul de date cu caracter personal numeşte o persoană responsabilă de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, subordonată nemijlocit conducătorului instituţiei, care nu va avea alte responsabilităţi incompatibile cu sarcinile funcţiei de implementare a politicii.

18. Persoana responsabilă de politica de securitate a datelor cu caracter personal va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

19. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere,

detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

20. Deţinătorii de date cu caracter personal întreprind următoarele acţiuni:

1) definesc clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală;

2) asigură măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal;

3) elaborează procedurile de clasificare a informaţiei care conţine date cu caracter personal astfel încît să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date;

instruiesc persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

21. Documentaţia referitoare la politica de securitate a datelor cu caracter personal este centralizată, completă, actualizată cu regularitate şi conţine cel puţin următoarele elemente:

1) identitatea persoanei responsabile de politica de securitate;

2) măsurile de securitate;

3) mecanismul de punere în aplicare a măsurilor de securitate;

4) nomenclatorul datelor cu caracter personal prelucrate, a localizării acestora şi a operaţiunilor efectuate asupra lor;

5) lista nominală a utilizatorilor, autorizaţi să acceseze datele cu caracter personal;

6) configurarea sistemului informaţional de date cu caracter personal şi a reţelei;

7) descrierea detaliată a criteriilor, în conformitate cu care sînt accesibile datele cu caracter personal prelucrate în registrul ţinut manual;

8) documentaţia tehnică cu privire la controalele de securitate;

9) orarul controalelor de securitate;

10) măsurile de detectare a cazurilor de acces şi/sau de prelucrare neautorizată a datelor cu caracter personal;

11) rapoarte despre incidentele de securitate.

IV. SECURITATEA MEDIULUI FIZIC ŞI A TEHNOLOGIILOR INFORMAŢIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Secţiunea 1

Autorizarea accesului fizic

22. Pentru categoria N-1.

Accesul în sediile/oficiile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare, cartele cu microprocesoare).

Conducătorii deţinătorilor de date cu caracter personal elaborează şi aprobă listele de acces, care se revizuiesc nu mai rar decît o dată în lună şi însemnele care autorizează accesul.

23. Suplimentar pentru categoria N-2.

Accesul se efectuează în baza cartelelor de identificare, cartelelor cu microprocesoare sau altor tehnologii identice

Secţiunea 2

Administrarea şi monitorizarea accesului fizic

24. Pentru categoria N-1.

Se efectuează administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces.

Înainte de acordarea accesului fizic la sistemele informaţionale de date cu caracter personal se verifică competenţele de acces.

Registrele de monitorizare se păstrează minimum un an, la expirarea căruia acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus

lichidării se transmit în arhivă.

25. Suplimentar pentru categoria N-2.

Încăperile unde sînt instalate sistemele informaţionale de date cu caracter personal se echipează cu sisteme de control al accesului şi supraveghere video, în scopul urmăririi accesului persoanelor în aceste spaţii.

În procesul monitorizării se utilizează mijloace de supraveghere şi alarmă în regim real de timp a tuturor cazurilor de acces autorizat şi/sau neautorizat.

Sînt utilizate mijloace automatizate care asigură identificarea cazurilor de acces neautorizat şi iniţierea acţiunilor de blocare a accesului.

Secţiunea 3

Securitatea sediilor/oficiilor/birourilor şi mijloacelor de prelucrare a datelor cu caracter personal

26. Pentru categoria N-1.

Perimetrul de securitate se determină concret şi clar. Perimetrul clădirii sau încăperii în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal trebuie să fie integru din punct de vedere fizic.

Pereţii exteriori ai încăperilor trebuie să fie rezistenţi, intrările echipate cu lacăte, mijloace de control al accesului, semnalizare etc.

În cazul amplasării încăperilor la parter şi/sau la ultimul etaj al clădirii, precum şi în cazul existenţei balcoanelor, scărilor antiincendiare, la ferestrele încăperilor respective se instalează gratii.

Computerele, serverele, alte terminale de acces trebuie amplasate în locuri cu acces limitat pentru persoane străine.

Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii.

Agendele şi/sau cărţile de telefoane în care se conţin indicii despre locul amplasării mijloacelor de prelucrare a datelor cu caracter personal nu vor fi accesibile persoanelor străine.

Amplasarea mijloacelor de prelucrare a datelor cu caracter personal trebuie să răspundă necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii deţinătorului de date cu caracter personal.

Purtătorii de informaţii şi mijloacele de prelucrare a datelor cu caracter personal scoase din încăperile aflate în perimetrul de securitate nu trebuie lăsate fără supraveghere în locuri publice.

27. Suplimentar pentru categoria N-2.

Se implementează sisteme de constatare a intruziunilor pentru uşile exterioare şi ferestrele amplasate în locuri accesibile.

Utilajul de rezervă şi purtătorii de informaţii care conţin date cu caracter personal se păstrează în locuri care permit evitarea distrugerilor sau deteriorărilor ca rezultat al calamităţilor în sediul/oficiul/biroul de bază.

Secţiunea 4

Controlul vizitatorilor

28. Pentru categoria N-1.

Trebuie asigurat controlul accesului fizic al vizitatorilor în încăperile unde sînt amplasate sistemele informaţionale de date cu caracter personal.

Accesul vizitatorilor se înregistrează în registre, care se păstrează minimum un an. La expirarea termenului de un an, registrele sînt lichidate, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

29. Suplimentar pentru categoria N-2.

Vizitatorii sistemelor informaţionale de date cu caracter personal trebuie să fie însoţiţi de persoane împuternicite în asemenea scop, cu exercitarea în paralel a controlului asupra acţiunilor acestora.

Secţiunea 5

Securitatea electroenergetică

30. Pentru categoria N-1.

Se asigură securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate.

În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, trebuie asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

Trebuie prevăzute surse autonome de alimentare cu energie electrică de scurtă durată, care sînt folosite pentru terminarea corectă a sesiunii de lucru a

sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

31. Suplimentar pentru categoria N-2.

Sînt prevăzute şi asigurate surse de alimentare cu energie electrică de lungă durată, care sînt folosite în cazul deconectării pentru perioade îndelungate şi necesităţii continuării îndeplinirii de către sistemele informaţionale de date cu caracter personal a sarcinilor funcţionale stabilite.

Secţiunea 6

Securitatea cablurilor de reţea

32. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Cablurile de reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, trebuie protejate contra conectărilor nesancţionate sau deteriorărilor.

Cablurile de tensiune trebuie separate de cele comunicaţionale, pentru a exclude bruiajul.

Deţinătorii de date cu caracter personal efectuează controale, nu mai rar decît odată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea.

Secţiunea 7

Asigurarea securităţii antiincendiare a sistemelor informaţionale de date cu caracter personal

33. Pentru categoria N-1.

Se prevăd mijloace de asigurare a securităţii antiincendiare a sediilor/oficiilor/birourilor unde sînt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

34. Suplimentar pentru categoria N-2.

Se implementează sisteme automatizate de depistare/semnalizare şi stingere a incendiilor în sediile/oficiile/birourile unde sînt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

Secţiunea 8

Controlul instalării şi scoaterii componentelor TI

35. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se exercită controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal.

Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.

Secţiunea 9

Măsurile generale de administrare a securităţii informaţionale

36. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.

Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.

Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.

Trebuie administrat accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal, sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii deţinătorului de date cu caracter personal.

Scoaterea şi introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează.

V. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

Secţiunea 1

Identificarea şi autentificarea utilizatorului

37. Pentru categoria N-1.

Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.

Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.

În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal, ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă sau se suspendă de către deţinătorul de date cu caracter personal.

38. Suplimentar pentru categoria N-2.

Se utilizează autentificarea multifactorială (complexă), care include parole şi mijloace fizice speciale de acces cu memorie ori cartele cu microprocesoare sau parole şi mijloace biometrice de autentificare.

Secţiunea 2

Identificarea şi autentificarea echipamentului

39. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal.

Secţiunea 3

Administrarea identificatorilor utilizatorilor

40. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator;

2) verificarea autenticităţii fiecărui utilizator;

3) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului;

4) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;

5) dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (inacţiune în perioada de maximum 2 luni);

6) executarea copiilor de arhivă a ID-urilor utilizatorilor.

Secţiunea 4

Administrarea mijloacelor de autentificare

41. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Deţinătorii de date cu caracter personal determină procedurile administrative, care reglementează procesul distribuirii şi ridicării mijloacelor de autentificare a utilizatorilor, inclusiv acţiunile în cazul pierderii/compromiterii sau defecţiunii acestora.

După instalarea sistemului, se schimbă informaţiile de autentificare a utilizatorilor utilizate standard.

Secţiunea 5

Asigurarea conexiunii bilaterale în cazul introducerii informaţiei de autentificare a utilizatorilor

42. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură conexiunea bilaterală a deţinătorului de date cu caracter personal cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

Secţiunea 6

Utilizarea parolelor în procesul asigurării securităţii informaţionale

43. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor, care includ:

1) păstrarea confidenţialităţii parolelor;

2) interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;

3) modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri ale sistemului sau parolei;

4) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere;

5) modificarea parolelor peste intervale de maximum 3 luni;

6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

Secţiunea 7

Administrarea parolelor utilizatorilor

44. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se folosesc identificatoare individuale pentru fiecare utilizator şi parole individuale ale acestora pentru asigurarea posibilităţii de stabilire a responsabilităţii.

Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora.

Se asigură blocarea accesului după trei tentative greşite de autentificare.

Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioada de un an) şi prevenirea folosirii repetate ale acestora.

La momentul introducerii, parolele nu se reflectă în clar pe monitor.

Parolele se păstrează în formă cifrată, utilizîndu-se algoritmul criptografic unilateral (funcţia hash).

VI. ADMINISTRAREA ACCESULUI UTILIZATORILOR

Secţiunea 1

Administrarea accesului

45. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se implementează mecanisme de înregistrare şi evidenţă a persoanelor care au acces sau participă la operaţiunile de prelucrare a datelor cu caracter personal şi care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

Secţiunea 2

Administrarea conturilor de acces (account-urilor)

6. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora.

Sînt folosite mijloace automatizate de suport în scopul administrării conturilor de acces.

Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp (pentru fiecare tip de cont de acces în parte).

Sînt dezactivate automat, după o perioadă de maximum trei luni, conturile de acces ale utilizatorilor neactivi, care prelucrează date cu caracter personal.

Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

Secţiunea 3

Acordarea accesului

47. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Este autorizat accesul la sistemele informaţionale de date cu caracter personal în conformitate cu politica de administrare a accesului stabilită de deţinătorul de date cu caracter personal.

Accesul la funcţiile de securitate ale sistemelor informaţionale de date cu caracter personal şi la datele acestora este acordat doar persoanelor responsabile indicate expres în politica de securitate a deţinătorului de date cu caracter personal.

Secţiunea 4

Revizuirea drepturilor de acces ale utilizatorilor

48. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Drepturile de acces ale utilizatorilor la sistemele informaţionale de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni) şi după oricare schimbare de statut al utilizatorului.

Secţiunea 5

Administrarea fluxurilor informaţionale

49. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se autorizează de către deţinătorii de date cu caracter personal realizarea fluxurilor informaţionale în procesul transmiterii acestora în interiorul şi în afara sistemelor informaţionale de date cu caracter personal.

Secţiunea 6

Repartizarea obligaţiilor şi învestirea cu minimul de drepturi şi competenţe

50. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Repartizarea obligaţiilor subiecţilor care asigură funcţionarea sistemelor informaţionale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competenţe corespunzătoare de acces, printr-un act administrativ al conducerii deţinătorului de date cu caracter personal.

Utilizatorii sistemelor informaţionale de date cu caracter personal se învestesc doar cu acele drepturi/competenţe, care sînt necesare pentru realizarea

de către ei a obiectivelor stabilite acestora.

Secţiunea 7

Informaţii de avertizare

51. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea sistemelor informaţionale de date cu caracter personal este controlată şi că folosirea neautorizată a acestora se urmăreşte în conformitate cu legislaţia.

Secţiunea 8

Blocarea sesiunii de lucru

52. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal, se blochează (la solicitarea utilizatorului sau automat, după maximum 15 minute de perioadă inactivă a utilizatorului), fapt care face imposibil accesul de mai departe pînă în momentul cînd utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

Secţiunea 9

Controlul administrării accesului

53. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se efectuează controlul acţiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Secţiunea 10

Marcarea documentelor

54. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Informaţia ieşită din sistem, care conţine date cu caracter personal, se marchează, indicîndu-se prescripţii pentru prelucrarea ulterioară şi răspîndirea acesteia, inclusiv indicîndu-se numărul de identificare unic al deţinătorului de

date cu caracter personal.

Secţiunea 11

Accesul de la distanţă

55. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal trebuie securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate, supuse monitorizării şi controlului.

Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de persoanele responsabile ale deţinătorilor de date cu caracter personal şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Secţiunea 12

Limitarea folosirii tehnologiilor fără fir

56. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal se stabilesc limitări şi se elaborează reguli de folosire a tehnologiilor fără fir care permit accesul la sistemele informaţionale de date cu caracter personal.

Accesul fără fir la sistemele informaţionale de date cu caracter personal este documentat, supus monitorizării şi controlului.

Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.

Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale deţinătorului de date cu caracter personal.

Secţiunea 13

Administrarea accesului echipamentului portativ şi mobil

57. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se stabilesc limitări şi se elaborează reguli de folosire a echipamentului portativ şi mobil care permit accesul la sistemele informaţionale de date cu caracter personal.

Accesul la sistemele informaţionale de date cu caracter personal cu folosirea

echipamentului portativ şi mobil se documentează, este monitorizat şi controlat.

Folosirea echipamentului portativ şi mobil este autorizată de persoanele responsabile ale deţinătorului de date cu caracter personal.

VII. PROTECŢIA SISTEMELOR INFORMAŢIONALE ŞI COMUNICAŢIILOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

Secţiunea 1

Divizarea programelor aplicative

58. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a sistemelor informaţionale de date cu caracter personal.

Secţiunea 2

Izolarea funcţiilor de securitate

59. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură izolarea funcţiilor de securitate de funcţiile care nu se atribuie la securitatea sistemelor informaţionale de date cu caracter personal.

Secţiunea 3

Informaţia restantă

60. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Trebuie preîntîmpinate tentativele dezvăluirii neautorizate sau neintenţionate a informaţiei restante care conţine date cu caracter personal, prin intermediul resurselor informaţionale general accesibile.

Secţiunea 4

Protecţia contra refuzului în serviciu

61. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură protecţia sistemelor informaţionale de date cu caracter personal sau limitate posibilităţile de realizare a atacurilor de diferite tipuri, inclusiv

DOS (denial of service) - „refuz în serviciu”.

Secţiunea 5

Priorităţile resurselor

62. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităţilor, a folosirii resurselor informaţionale în care sînt prelucrate date cu caracter personal.

Secţiunea 6

Protecţia perimetrului sistemelor informaţionale în care sîntprelucrate date cu caracter personal

63. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se efectuează monitorizarea permanentă şi controlul comunicaţiilor la perimetrul exterior al sistemelor informaţionale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaţionale.

Amplasarea resurselor general accesibile se asigură în spaţiile special destinate a reţelei de calcul cu interfeţele fizice de reţea.

Este asigurată imposibilitatea accesului din exterior a utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal.

Secţiunea 7

Asigurarea integrităţii datelor cu caracter personal transmise

64. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură integritatea datelor cu caracter personal transmise, utilizîndu-se mijloacele de protecţie criptografică şi semnătura digitală.

Secţiunea 8

Asigurarea confidenţialităţii datelor cu caracter personal transmise

65. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură confidenţialitatea datelor cu caracter personal transmise,

utilizîndu-se mijloace de protecţie criptografică a informaţiei.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE INFORMAŢIONALE D DATE CU CARACTER PERSONAL

Secţiunea 1

Generarea înregistrărilor de audit în sistemele informaţionale e date cu caracter personal

66. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Deţinătorii de date cu caracter personal organizează generarea înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

Secţiunea 2

Lista evenimentelor înregistrate de sistemul de audit a securităţii în sistemele informaţionale de date cu caracter personal

67. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

1) Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:

a) data şi timpul tentativei intrării/ieşirii;

b) ID-ul utilizatorului;

c) rezultatul tentativei de intrare/ieşire – pozitivă sau negativă.

2) Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:

a) data şi timpul tentativei de pornire;

b) denumirea/identificatorul programului aplicativ sau procesului;

c) ID-ul utilizatorului;

d) rezultatul tentativei de pornire – pozitivă sau negativă.

3) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);

b) denumirea (identificatorul) aplicaţiei sau procesului;

c) ID-ul utilizatorului;

d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);

e) tipul operaţiunii solicitate (citire, înregistrare ştergere etc.);

f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

4) Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

a) data şi timpul modificării competenţelor;

b) ID-ul administratorului care a efectuat modificările;

c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

5) Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

a) data şi timpul eliberării;

b) denumirea informaţiei şi căile de acces la aceasta;

c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);

d) ID-ul utilizatorului, care a solicitat informaţia;

e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

Secţiunea 3

Prelucrarea rezultatelor auditului securităţii în sistemele informaţionale de date cu caracter personal

68. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

În caz de deranjament al auditului securităţii în sistemele informaţionale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal şi întreprinse măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

Secţiunea 4

Monitorizarea, analiza şi generarea rapoartelor de audit a securităţii în sistemele informaţionale de date cu caracter personal

69. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal

Se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal, în scopul depistării activităţilor neobişnuite sau suspecte de utilizare a acestor sisteme informaţionale, cu întocmirea raportului referitor la cazurile depistării acestor activităţi, stocate în mijloacele electronice de calcul şi întreprinderea acţiunilor prestabilite în politica de securitate pentru astfel de cazuri.

Secţiunea 5

Protejarea datelor de audit a securităţii în sistemele informaţionale de date cu caracter personal

70. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Rezultatele auditului securităţii în sistemele informaţionale de date cu caracter personal, care reprezintă operaţiuni de prelucrare a datelor cu caracter personal şi mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidenţialităţii şi integrităţii acestora.

Secţiunea 6

Păstrarea datelor de audit a securităţii în sistemele informaţionale de date cu caracter personal

71. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Durata stocării rezultatelor auditului securităţii în sistemele informaţionale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar în orice caz acest termen nu este mai mic de 2 ani, pentru a fi

posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare.

În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI A TEHNOLOGIILOR INFORMAŢIONALE

Secţiunea 1

Înlăturarea deficienţelor de soft destinat prelucrării datelor cu caracter personal

72. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor soft-uri.

Secţiunea 2

Asigurarea protecţiei contra programelor dăunătoare (viruşilor)

73. Pentru categoria N-1.

Se asigură protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

74. Suplimentar pentru categoria N-2.

Se asigură administrarea centralizată a mecanismelor de protecţie contra programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal.

Secţiunea 3

Tehnologiile şi mijloacele de constatare a intruziunilor

75. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se utilizează tehnologii şi mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaţionale de date cu caracter personal şi constatarea atacurilor, inclusiv care asigură identificarea tentativelor

folosirii neautorizate a sistemelor informaţionale.

Secţiunea 4

Asigurarea integrităţii soft-urilor şi informaţiei

76. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură protecţia şi posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal şi informaţiei care conţine date cu caracter personal.

Soft-urile destinate prelucrării datelor cu caracter personal şi informaţia care conţine date cu caracter personal, accesul la care se efectuează prin intermediul sistemelor de acces public, sînt securizate prin metoda folosirii semnăturii digitale.

Secţiunea 5

Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

77. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

X. COPIILE DE REZERVĂ ŞI RESTABILIREA INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI IT

Secţiunea 1

Copiile de rezervă ale informaţiei care conţine date cu caracter

78. Pentru categoria N-1.

Reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către deţinătorul de date cu caracter personal intervalul de timp în care se execută copiile de siguranţă a informaţiilor care conţin date cu caracter personal şi soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, dar în orice caz acest termen este mai mic de un an, care se păstrează în locuri protejate, în afara zonei de amplasare a acestei informaţii şi soft-urile de bază.

Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei care conţine date cu caracter personal.

Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

79. Suplimentar pentru categoria N-2.

Copiile de siguranţă se păstrează în cutii metalice cu sigiliu aplicat şi stocate în afara zonei de amplasare a informaţiei care conţine date cu caracter personal de soft-urile de bază sau, dacă este posibil, în încăperi din altă clădire.

Se identifică potenţialele probleme de acces în locurile de păstrare a copiilor de siguranţă în cazul defectului sau avariei şi se determină acţiunile concrete pentru restabilirea căilor de acces.

Secţiunea 2

Serviciile telecomunicaţionale de rezervă

80. Pentru categoria N-2.

Se identifică serviciile telecomunicaţionale de bază şi de rezervă, inclusiv se soluţionează întrebările privind folosirea serviciilor telecomunicaţionale de rezervă în scopul restabilirii accesibilităţii serviciilor de bază ale sistemelor informaţionale de date cu caracter personal.

Furnizorii serviciilor telecomunicaţionale de bază şi de rezervă urmează a fi diferiţi pentru a nu fi supuşi pericolelor comune.

XI. CONTROALELE DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

81. Deţinătorii de date cu caracter personal verifică cu regularitate, cel puţin odată pe an, îndeplinirea măsurilor tehnice şi/sau organizaţionale luate pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea în procesul prelucrării datelor cu caracter personal a sistemelor de telecomunicaţii şi/sau efectuarea îmbunătăţirilor, în caz de necesitate.

82. Controalele de securitate sînt actualizate de fiecare dată cînd deţinătorul de date cu caracter personal este reorganizat sau îşi schimbă infrastructura.83. În scopul verificării nivelului de protecţie a sistemelor informaţionale de date cu caracter personal, precum şi în scopul preîntîmpinării unor eventuale cazuri de acces ilicit sau întîmplător asupra acestor sisteme informaţionale, depistării locurilor slabe în mecanismele de protejare a acestora, Centrul întreprinde periodic controale de securitate, inclusiv cu efectuarea unor măsuri tehnice speciale pentru simularea unui model de accesare a sistemelor informaţionale de date cu caracter personal.

84. Rezultatele controalelor efectuate de Centru sînt puse imediat la dispoziţia deţinătorului de date cu caracter personal, nivelul de protecţie a sistemelor informaţionale de date cu caracter personal a căruia a servit obiect al controlului, cu prescrierea, în caz de necesitate, a acţiunilor necesare de a fi întreprinse în vederea asigurării securităţii prelucrării datelor cu caracter personal.

XII. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

Secţiunea 1

Instructajul de reacţionare la incidentele de securitate a sistemelor informaţionale de date cu caracter personal

85. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.

Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal trece, minimum odată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

Secţiunea 2

Prelucrarea incidentelor de securitate a sistemelor informaţionale de date cu caracter personal

86. Pentru categoria N-1.

Este asigurat mecanismul de informare neîntîrziată a conducerii deţinătorului de date cu caracter personal despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

87. Suplimentar pentru categoria N-2.

Trebuie utilizate mijloace automatizate pentru susţinerea procesului de prelucrare a incidentelor de securitate a sistemelor informaţionale de date cu caracter personal.

Secţiunea 3

Monitorizarea incidentelor de securitate a sistemelor informaţionale de date cu caracter personal

88. Pentru categoria N-1.

Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent.

89. Suplimentar pentru categoria N-2.

Sînt utilizate mijloace automatizate pentru urmărirea incidentelor de securitate a sistemelor informaţionale de date cu caracter personal, colectarea şi analiza informaţiei despre aceste incidente.

Secţiunea 4

Prezentarea rapoartelor despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal

90. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal.Anual, către 31 ianuarie, deţinătorii de date cu caracter personal prezintă Centrului raportul generalizat despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal. În baza acestui raport, Centrul întreprinde măsurile ce se impun de Legea cu privire la protecţia datelor cu caracter personal.

XIII. PROTECŢIA TEHNICĂ A INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL

91. Pentru categoria N-2.

Este exclusă prezenţa necontrolată a persoanelor sau a mijloacelor de transport, precum şi instalarea întîmplătoare a antenelor, într-o zonă de minimum 15 metri de la locul amplasării mijloacelor tehnice principale ale sistemului informaţional de date cu caracter personal (în continuare – perimetru controlat), în scopul asigurării securităţii prelucrării datelor cu caracter personal.

Încăperile pentru servere se protejează contra scurgerii informaţiei care conţine date cu caracter personal din cauza emisiilor electromagnetice prin ecranarea încăperilor sau instalarea sistemelor de bruiaj electromagnetic, care se proiectează, realizează şi cercetează de întreprinderi specializate în domeniu.

În cazul ecranării încăperilor în care se află mijloacele tehnice de prelucrare a datelor cu caracter personal, este asigurată continuitatea conexiunii electrice a materialului tuturor părţilor ecranului: pereţi, tavan, podea, ferestre şi uşi.

Construcţiile de ecranare trebuie să posede prize de pămînt care se amplasează în perimetrul controlat.

Trebuie asigurată protecţia informaţiei care conţine date cu caracter personal contra scurgerii prin intermediul reţelei electrice, inclusiv încrucişarea reţelelor electrice ale obiectului cu instalarea filtrelor de protecţie care să blocheze (bruieze) semnalul.

Se exclude sau se limitează instalarea neautorizată a altor dispozitive electrice, radio sau de alt gen în încăperile unde sînt amplasate mijloacele tehnice de prelucrare a datelor cu caracter personal, în scopul asigurării securităţii prelucrării datelor cu caracter personal.

Utilajul, liniile căruia au ieşire în afara perimetrului controlat, este instalat la o distanţă de cel puţin 3 metri de la mijloacele TI în care sînt prelucrate date cu caracter personal.

XIV. SPECIFICUL CERINŢELOR DE SECURITATE

ÎN CAZUL FORMEI MANUALE DE ŢINERE A REGISTRELOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

92. Prevederile prezentelor Cerinţe, cu excepţia pct.11-13, 23, 25, 27, 30-32, 35, 37-44, 46, 49, 51-53, 55-68, 72-77, 80, 87-89 şi 91, se aplică corespunzător de către deţinătorii de date cu caracter personal în cazul formei manuale de ţinere a registrelor în care sînt prelucrate seriile structurate de date cu caracter personal, accesibile conform criteriilor centralizate sau descentralizate, ori repartizate conform criteriilor funcţionale sau geografice.

93. Totodată, înregistrările de audit a securităţii registrelor ţinute manual în care sînt prelucrate date cu caracter personal, trebuie să conţină:

1) numele şi prenumele utilizatorului;

2) numele fişei accesate (pagina şi inscripţia din registru);

3) numărul înregistrărilor efectuate;

4) tipul de acces;

5) data accesului (an, lună, zi);

6) timpul (ora, minuta) şi durata accesului.

Anexa nr.1

la Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal

CATEGORIILE DE DATE CU CARACTER PERSONAL

1. Datele cu caracter personal, care direct sau indirect identifică o persoană fizică, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale, se împart în două categorii: obişnuite şi speciale.

2. Categoria specială a datelor cu caracter personal o constituie informaţia care dezvăluie originea rasială sau etnică, convingerile politice, religioase, privind starea de sănătate sau viaţa intimă, precum şi cele privind condamnările penale ale unei persoane fizice.

3. Categoria obişnuită o constituie informaţia care dezvăluie:

1) numele şi prenumele;

2) sexul;

3) data şi locul naşterii;

4) cetăţenia;

5) IDNP;

6) imaginea;

7) vocea;

8) situaţia familială;

9) situaţia militară;

10) datele de geolocalizare/datele de trafic;

11) porecla/pseudonimul;

12) datele personale ale membrilor de familie;

13) datele din permisul de conducere;

14) datele din certificatul de înmatriculare;

15) situaţia economică şi financiară;

16) datele privind bunurile deţinute;

17) datele bancare;

18) semnătura;

19) datele din actele de stare civilă;

20) numărul dosarului de pensie;

21) codul personal de asigurării sociale (CPAS);

22) codul asigurării medicale (CPAM);

23) numărul de telefon/fax;

24) numărul de telefon mobil;

25) adresa (domiciliului/reşedinţei);

26) adresa e-mail;

27) datele genetice;

28) datele biometrice şi antropometrice;

29) datele dactiloscopice;

30) profesia şi/sau locul de muncă;

31) formarea profesională – diplome – studii;

32) obişnuinţele/preferinţele/comportamentul;

33) caracteristicile fizice.

4. În cazul prelucrării categoriei obişnuite de date cu caracter personal, deţinătorii de date cu caracter personal includ în politica de securitate a datelor cu caracter personal şi implementează cerinţele stabilite pentru nivelul unu de securitate a sistemelor informaţionale de date cu caracter personal – (N – 1).

5. În cazul prelucrărilor categoriei speciale de date cu caracter personal, deţinătorii de date cu caracter personal, suplimentar cerinţelor stabilite pentru nivelul unu de securitate, includ în politica de securitate a datelor cu caracter personal şi implementează cerinţele stabilite pentru nivelul doi de securitate a sistemelor informaţionale de date cu caracter personal – (N – 2).

PARLAMENTUL

COD *Nr. 1107 din 06-06-2002*

CODUL CIVIL AL REPUBLICII MOLDOVA

Publicat : 22-06-2002 în Monitorul Oficial Nr. 82-86 art. 661

**Republicat în Monitorul Oficial nr.66-75 din 01.03.2019 art.132*

Articolul 476. Obiectele de proprietate intelectuală

(1) Se consideră obiect de proprietate intelectuală orice rezultat al activității intelectuale, confirmat și protejat prin drepturile corespunzătoare privind utilizarea acestuia.

(2) Obiectele de proprietate intelectuală se divizează în două categorii:

a) obiecte de proprietate industrială (invenții, soiuri de plante, topografii de circuite integrate, mărci, desene și modele industriale, indicații geografice, denumiri de origine și specialități tradiționale garantate);

b) obiecte ale dreptului de autor (opere literare, artistice și științifice etc.) și ale drepturilor conexe (interpretări, fonograme, videograme și emisiuni ale organizațiilor de difuziune etc.).

(3) De domeniul proprietății intelectuale țin și alte bunuri ce dispun de un sistem de reglementare separat, cum ar fi:

a) secretul comercial (know-how);

b) numele comercial.

(4) În cazul obiectelor de proprietate industrială, dreptul asupra acestora apare în urma înregistrării obiectului, a acordării titlului de protecție de către oficiul național de proprietate intelectuală sau în alte condiții prevăzute de legislația națională, precum și în baza tratatelor internaționale la care Republica Moldova este parte. În cazul obiectelor dreptului de autor și ale drepturilor conexe, înregistrarea nu este o condiție obligatorie pentru apariția și exercitarea drepturilor respective, aceste obiecte fiind protejate din momentul creării lor.

(5) În condițiile legii, titularul dreptului asupra obiectului de proprietate intelectuală:

a) poate înstrăina dreptul prin cesiune;

b) poate permite exploatarea lui de către terți prin licență exclusivă sau neexclusivă;

c) poate exercita alte drepturi morale şi patrimoniale prevăzute de lege în privinţa obiectului dreptului exclusiv.

(6) Cu excepţiile prevăzute de lege, nicio persoană nu poate exploata dreptul asupra obiectului de proprietate intelectuală al altuia fără licenţa corespunzătoare. Licenţa se prezumă neexclusivă dacă nu s-a prevăzut expres contrariul.

(7) Dreptul asupra obiectului de proprietate intelectuală şi dreptul acordat prin licenţă se consideră bunuri incorporale şi pot fi grevate cu drepturi reale limitate în folosul terţilor.

Articolul 477. Conţinutul digital şi bunul digital

(1) Conţinut digital se consideră datele produse şi livrate în formă digitală, cum sînt programele de calculator, aplicaţiile, jocurile, muzica, înregistrările video sau textele, indiferent dacă sînt accesate prin descărcare sau prin flux continuu, de pe un suport material sau prin orice alte mijloace.

(2) Dacă un conţinut digital este livrat pe un suport material, cum sînt CD-urile sau DVD-urile, lui i se aplică dispoziţiile privind bunurile corporale.

(3) Bun digital al unei persoane se consideră:

a) conţinutul digital la care ea are dreptul;

b) contul la o poştă electronică, la o reţea sau alt cont online, la care ea are dreptul.

(4) Custodele bunului digital este profesionistul care oferă acces, menţine, procesează, primeşte sau păstrează bunul digital al unei alte persoane (utilizator), conform contractului dintre custode şi utilizator.

Articolul 478. Accesul terţilor la bunurile digitale

(1) Utilizatorul poate folosi serviciul electronic oferit de custodele bunului digital pentru a ordona custodelui să ofere acces sau să nu ofere acces la toate sau anumite bunuri digitale, inclusiv la conţinutul comunicărilor electronice. Dacă serviciul respectiv oferit de custode permite utilizatorului să modifice sau să revoce un ordin în orice moment, ordinul privind oferirea accesului are prioritate faţă de voinţa exprimată de utilizator într-un testament sau într-un mandat.

(2)Dacă utilizatorul nu a folosit serviciul prevăzut la alin.(1) sau dacă custodele nu oferă un asemenea serviciu, utilizatorul poate permite sau interzice, printr-un testament sau mandat, accesul anumitor persoane determinate sau determinabile la toate sau anumite bunuri digitale.

(3) Ordinul dat de utilizator conform alin. (1) sau (2) are prioritate faţă de condiţiile contractului dintre custode şi utilizator. În absenţa unui ordin al utilizatorului conform alin. (1) sau (2), se aplică condiţiile contractului dintre custode şi utilizator, care pot permite, limita sau exclude accesul terţilor interesaţi la bunurile digitale ale utilizatorului.

(4) În cazul în care în privința utilizatorului a fost instituită o măsura de ocrotire judiciară, iar ocrotitorul provizoriu, curatorul sau tutorele nu are acces la bunurile digitale ale persoanei ocrotite conform alin. (1), (2) sau (3), el poate cere de la instanța de judecată să-i fie acordat dreptul la acces dacă are un interes legitim în acest sens și dacă aceasta nu contravine dorințelor și sentimentelor exprimate în trecut și prezent de către persoana ocrotită. În aceleași condiții, instanța de judecată poate acorda dreptul la acces prin hotărîrea judecătorească prin care se instituie măsura de ocrotire judiciară.

(5) Custodele care trebuie să ofere acces la bunurile digitale conform alin. (1)-(4) îl poate oferi prin:

a) acces deplin la contul online;

b) acces parțial la contul online, dar suficient pentru a respecta împuternicirile persoanei îndreptățite;

c) furnizarea către persoana îndreptățită a copiilor, pe un suport durabil, de pe bunurile digitale pe care utilizatorul le-ar fi putut accesa.

(6) Custodele poate stabili o taxă rezonabilă pentru a acoperi costurile de procesare a cererii și de oferire a accesului.

(7) Custodele nu este obligat să ofere acces la bunurile digitale șterse de către utilizator.

(8) Dispozițiile prezentului articol nu aduc atingere altor dispoziții legale care permit terților accesul la bunurile digitale ale unei persoane.

Secțiunea a 3-a
Răspunderea pentru dobîndirea, utilizarea sau divulgarea ilegală a secretelor comerciale

Articolul 2047. Răspunderea pentru dobîndirea, utilizarea sau divulgarea legală a secretelor comerciale

(1) Cel care a dobîndit, a utilizat sau a divulgat în mod ilegal un secret comercial (făptuitor) este obligat să repare prejudiciul patrimonial și moral cauzat persoanei fizice sau juridice care deține controlul legal asupra acelui secret comercial (deținător al secretului comercial), în condițiile prezentei secțiuni.

(2) Deținătorul secretului comercial are dreptul să exercite mijloacele juridice de apărare prevăzute de prezenta secțiune și de alte dispoziții legale pentru a preveni dobîndirea, utilizarea sau divulgarea ilegală a secretelor lui comerciale sau pentru a obține reparație în urma unor astfel de fapte.

(3) În sensul prezentei secțiuni, se consideră secrete comerciale informațiile care îndeplinesc cumulativ următoarele cerințe:

a) sînt secrete în sensul că nu sînt, ca întreg sau astfel cum se prezintă sau

se articulează elementele acestora, cunoscute la nivel general sau ușor accesibile persoanelor din cercurile care se ocupă, în mod normal, de tipul de informații în cauză;

b) au valoare comercială prin faptul că sînt secrete;

c) au făcut obiectul unor măsuri rezonabile, în circumstanțele date, luate de către persoana care deține în mod legal controlul asupra informațiilor respective, pentru a fi păstrate secrete.

(4) În cazul în care autorizarea comercializării produselor farmaceutice sau a produselor chimice pentru agricultură care conțin preparate chimice noi este condiționată de comunicarea de date nedivulgabile rezultate din încercări sau de alte date nedivulgabile a căror stabilire cere un efort considerabil, aceste date sînt protejate atît contra exploatării lor neloiale în comerț, cît și contra divulgării, cu excepția cazurilor cînd divulgarea este necesară pentru protecția publicului sau cînd sînt luate măsuri pentru a asigura protejarea datelor respective contra exploatării lor neloiale în comerț.

Articolul 2048. Dobîndirea, utilizarea și divulgarea legală de secrete comerciale

(1) Dobîndirea unui secret comercial este considerată legală în cazul în care secretul comercial este obținut prin oricare dintre următoarele mijloace:

a) descoperirea sau crearea independentă;

b) analiza, studierea, dezasamblarea sau testarea unui produs sau a unui obiect care a fost făcut public sau care se află în mod legal în posesia celui care a dobîndit informațiile și căruia nu i se aplică nicio obligație valabilă din punct de vedere legal de a limita dobîndirea secretului comercial;

c) exercitarea dreptului salariaților sau al reprezentanților salariaților la informare și la consultare în conformitate cu legislația;

d) orice altă practică care, în circumstanțele date, este conformă cu practicile comerciale loiale.

(2) Dobîndirea, utilizarea sau divulgarea unui secret comercial este considerată legală în măsura în care o astfel de dobîndire, utilizare sau divulgare este impusă sau permisă în temeiul legislației.

Articolul 2049. Dobîndirea, utilizarea și divulgarea ilegală de secrete comerciale

(1) Dobîndirea unui secret comercial fără consimțămîntul deținătorului secretului comercial este considerată ilegală ori de cîte ori este efectuată prin:

a) accesul neautorizat, însușirea sau copierea oricăror documente, obiecte, materiale, substanțe sau fișiere electronice care se află în mod legal sub con-

trolul deținătorului secretului comercial și care conțin secretul comercial sau din care poate fi dedus secretul comercial;

b) orice alt comportament care, în circumstanțele date, contravine practicilor comerciale loiale.

(2) Utilizarea sau divulgarea unui secret comercial este considerată ilegală ori de cîte ori este săvîrșită, fără consimțămîntul deținătorului secretului comercial, de către o persoană care îndeplinește oricare dintre următoarele condiții:

a) a dobîndit secretul comercial în mod ilegal;

b) încalcă un contract de confidențialitate sau orice altă obligație de a nu divulga secretul comercial;

c) încalcă o obligație contractuală sau de altă natură care limitează utilizarea secretului comercial.

(3) Dobîndirea, utilizarea sau divulgarea unui secret comercial este, de asemenea, considerată ilegală atunci cînd o persoană, în momentul dobîndirii, utilizării sau divulgării, avea cunoștință sau ar fi trebuit să aibă cunoștință, în circumstanțele date, de faptul că secretul comercial a fost obținut, direct sau indirect, de la o altă persoană care a utilizat sau a divulgat secretul comercial în mod ilegal în sensul alin. (2).

(4) Producerea, oferirea sau introducerea pe piață a mărfurilor care încalcă secretul comercial ori importul, exportul sau depozitarea unor astfel de mărfuri în aceste scopuri este, de asemenea, considerată drept o utilizare ilegală a unui secret comercial atunci cînd persoana care desfășoară astfel de activități avea cunoștință sau ar fi trebuit să aibă cunoștință, în circumstanțele date, de faptul că secretul comercial a fost utilizat în mod ilegal în sensul alin. (2).

(5) În sensul prezentei secțiuni, se consideră mărfuri care încalcă secretul comercial mărfurile a căror concepere, caracteristici, funcționare, proces de producție sau comercializare beneficiază în mod semnificativ de secrete comerciale dobîndite, utilizate sau divulgate în mod ilegal.

Secretul profesional

Denumirea generală pentru un grup de secrete protejate de lege, necesitatea de protejare rezultă din confidențialitatea informației posedate în activitate sau de altă natură a profesiilor individuale. De exemplu, secretele profesionale includ, în special, privilegiile avocat-client, secretele medicale și secretele notariale. Un secret profesional trebuie să se distingă de un secret oficial, obligația de a respecta confidențialitatea rezultă din interesul de serviciu.

PARLAMENTUL

LEGEA Nr. 1260 din 19-07-2002

cu privire la avocatură

Publicat : 12-09-2002 în Monitorul Oficial Nr. 126-127 art. 1001

MODIFICAT LP146 din 16.07.20, MO194-197/31.07.20 art.394; în vigoare 31.07.20

Articolul 1. Noţiunea profesiei de avocat

(1) Profesia de avocat este exercitată de persoane calificate şi abilitate, conform legii, să pledeze şi să acţioneze în numele clienţilor lor, să practice dreptul, să apară în faţa unei instanţe judecătoreşti sau să consulte şi să reprezinte în materie juridică clienţii lor.

(2) Profesia de avocat este liberă şi independentă, cu organizare şi funcţionare autonomă, în condiţiile prezentei legi şi ale statutului profesiei de avocat. Activitatea avocatului nu este activitate de întreprinzător.

Articolul 2. Reglementarea activităţii de avocat

Reglementarea activităţii de avocat constă în:

a) stabilirea condiţiilor de bază şi a modului de acordare a asistenţei juridice profesionale persoanelor fizice şi juridice în Republica Moldova;

b) determinarea formelor de organizare a activităţii de avocat;

c) stabilirea genurilor de asistenţă juridică;

d) stabilirea garanţiilor pentru activitatea de acordare a asistenţei juridice calificate;

e) stabilirea modului de admitere în profesia de avocat.

Articolul 3. Principiile avocaturii

Avocatura se bazează pe următoarele principii:

a) asigurarea dreptului la apărare garantat de Constituţie;

b) libertate şi independenţă în activitatea de avocat;

c) democratism şi colegialitate în raporturile dintre avocaţi;

d) apartenenţă benevolă la asociaţiile profesionale de avocaţi;

e) asigurarea legalităţii şi umanismului.

Articolul 4. Cadrul juridic al activităţii de avocat

Cadrul juridic al activităţii de avocat se constituie din Constituţia Republicii Moldova, prezenta lege, alte legi care reglementează activitatea menţionată din statutul profesiei de avocat, precum şi din tratatele internaţionale la care Republica Moldova este parte.

Articolul 5. Dreptul la asistenţă juridică calificată

(1) Orice persoană are dreptul să îşi aleagă în mod liber avocatul pentru a fi consultată şi reprezentată de acesta în materie juridică.

(2) Statul asigură accesul la asistenţa juridică calificată tuturor persoanelor în condiţiile prezentei legi.

(3) Persoanele fizice şi juridice sînt în drept să beneficieze, în modul stabilit, de asistenţa juridică a oricărui avocat în bază de acord al părţilor.

(4) În cazurile prevăzute de lege, plata pentru asistenţa juridică calificată se achită de la bugetul de stat.

(5) Pornind de la starea materială a persoanei, avocatul îi poate acorda acesteia asistenţă juridică în mod gratuit.

(6) Avocaţii din Republica Moldova sînt în drept să îndeplinească unele delegaţii sau să exercite profesia de avocat în alte state, dacă aceasta este prevăzut de legislaţia statului respectiv.

Articolul 6. Exercitarea profesiei de avocat de către avocaţii din alte state

(1) Avocaţii din alte state pot exercita profesia de avocat pe teritoriul Republicii Moldova dacă întrunesc condiţiile prevăzute de lege, cu excepţia condiţiei privind deţinerea cetăţeniei.

(2) Avocatul din alt stat poate desfăşura activitate pe teritoriul Republicii Moldova dacă certifică calitatea de avocat în statul său de origine şi este înscris în registrul special ţinut de Consiliul Uniunii Avocaţilor din Republica Moldova, denumită în continuare Uniunea Avocaţilor.

(3) Avocatul din alt stat nu poate reprezenta interesele persoanelor fizice sau juridice în instanţele de judecată şi în relaţiile cu alte autorităţi publice decît în arbitrajul comercial internaţional. În cazul cînd interesele clientului o cer, precum şi la solicitarea acestuia, avocatul din alt stat poate asista avocatul din Republica Moldova.

(4) Avocatul din alt stat poate desfăşura activitate în cadrul cabinetului avocatului sau în cadrul biroului asociat de avocaţi în bază de contract.

(5) Registrul avocaţilor din alte state care au dreptul să exercite profesia de avocat pe teritoriul Republicii Moldova se publică pe pagina oficială de Internet a Uniunii Avocaţilor.

Articolul 7. Acordarea asistenţei juridice garantate de stat

Condiţiile, volumul şi modul de acordare de către avocaţi a asistenţei juridice garantate de stat se stabilesc prin Legea cu privire la asistenţa juridică garantată de stat.

Articolul 8. Genurile de asistenţă juridică calificată

(1) Avocaţii acordă persoanelor fizice şi juridice următoarele genuri de asistenţă juridică calificată:

a) oferă consultaţii şi explicaţii, expun concluzii cu privire la problemele juridice, prezintă informaţii verbale şi în scris referitoare la legislaţie;

b) întocmesc documente cu caracter juridic;

c) reprezintă interesele lor în instanţele de judecată;

d) reprezintă interesele lor în materie juridică în relaţiile cu autorităţile publice, notarii publici, executorii judecătoreşti şi cu alte persoane fizice şi juridice;

e) participă la urmărirea penală şi la dezbateri judiciare în cauzele penale în calitate de apărător sau reprezentant al victimei, al părţii civile, al părţii civilmente responsabile şi al martorilor;

f) desfăşoară activitate de fiduciar.

(2) Acordarea asistenţei juridice calificate prevăzute la alin. (1) lit.c) şi e) de către o persoană fizică sau juridică care nu are calitatea de avocat se pedepseşte, dacă legea nu prevede altfel.

(3) Avocaţii acordă persoanelor fizice şi juridice şi alte genuri de asistenţă juridică, neinterzise de lege, atît în cazul unor delegaţii unice, cît şi în cazul delegaţiilor pe termen lung.

(4) În procedura de acordare a asistenţei juridice, avocatul poate adeveri copii şi extrase din acte şi poate certifica semnăturile de pe actele necesare pentru acordarea asistenţei juridice. Avocatul nu poate efectua aceste acţiuni pentru sine, pentru membrii familiei sale, pentru rude sau afini.

(5) Acţiunile specificate la alin. (4) se certifică prin semnătura şi ştampila avocatului, în cazul în care dispune de aceasta, cu indicarea datei şi menţionarea corespunderii cu originalul.

Articolul 55. Secretul profesional

(1) Avocatul nu este în drept să divulge informaţiile confidenţiale ce i-au fost comunicate în timpul acordării asistenţei juridice, precum şi să transmită, fără acordul clientului, unor terţi documentele legate de exercitarea delegaţiei. (2) Obligaţia de a păstra secretul profesional nu este limitată în timp.

PARLAMENTUL

LEGEA Nr. 69 din 14-04-2016

cu privire la organizarea activităţii notarilor

Publicat : 26-08-2016 în Monitorul Oficial Nr. 277-287 art. 588

MODIFICAT LP246 din 15.11.18, MO30-37/01.02.19 art.89

Articolul 1. Domeniul de reglementare

(1) Prezenta lege stabileşte principiile de exercitare a activităţii notarilor, statutul notarului şi al notarului stagiar, modalităţile de organizare şi autoadministrare a notarilor, precum şi modalităţile de control al activităţii acestora.

(2) Procedura de îndeplinire a actelor notariale şi metodologia de calcul al plăţilor notariale sînt reglementate prin legi separate.

Articolul 2. Principiile exercitării activităţii de notar

Activitatea notarului se bazează pe următoarele principii:

a) principiul legalităţii;

b) principiul independenţei şi imparţialităţii;

c) principiul îndeplinirii personale a atribuţiilor;

d) principiul păstrării secretului profesional;

e) principiul nediscriminării.

Articolul7. Secretulprofesional

(1) Notarul este obligat să păstreze secretul profesional cu privire la actele îndeplinite şi faptele ce i-au devenit cunoscute în cadrul activităţii sale, indiferent de modul de obținere ori sursa informației, inclusiv după încetarea activității sale.

(2) Informaţii cu privire la actele notariale îndeplinite se pun la dispoziția:

a) persoanei în numele căreia aceste acte au fost îndeplinite sau reprezentantului acesteia. Informația cu privire la testament se eliberează doar la cererea personală a testatorului, iar terţilor – numai după decesul testatorului, în modul stabilit de legislație, dacă testatorul nu a degrevat notarul de obligația de a păstra secretul profesional;

b) instanţei de judecată, la prezentarea încheierii judecătorului, procuraturii și organelor de urmărire penală, în baza ordonanței acestor organe și cu autorizarea judecătorului de instrucție, în legătură cu cauzele penale, civile sau contravenționale aflate în curs de examinare;

c) organelor de control asupra activităţii notariale, în limita controlului efectuat;

d) executorului judecătoresc, în legătură cu procedura de executare ce ține de dosarele succesorale instrumentate de notari;

e) Serviciului Fiscal de Stat, conform normelor stabilite de lege.

(3) Pînă la intentarea cauzei penale sau contravenţionale, notarul va prezenta

informația privind înregistrarea sau neînregistrarea actului ori a acțiunii notariale în registrul actelor notariale, la cererea procuraturii sau a organului de urmărire penală, cu prezentarea obligatorie de către acesta a informației privind numărul de înregistrare, data înregistrării, solicitantul actului notarial şi tipul actului notarial.

(4) Persoanele cărora le-au devenit cunoscute informații deținute de notar în legătură cu îndeplinirea obligațiilor lor de serviciu sau de muncă sînt obligate să păstreze confidențialitatea acestor informații. Nerespectarea obligației respective atrage răspundere disciplinară și civilă.

(5) Notarul nu are obligația de a păstra secretul profesional şi poate oferi informațiile deținute în următoarele cazuri:

a) existența consimțământului scris al solicitantului actului notarial, expus în documentul notarial sau într-un alt document. Acest consimțământ poate fi exprimat de reprezentantul solicitantului sau, în caz de deces al solicitantului, de succesorii acestuia;

b) în cadrul unui proces intentat de către solicitantul actului notarial împotriva notarului, în temeiul încheierii instanței de judecată.

(6) Eliberarea de obligația de a păstra secretul profesional se aplică în cazul în care comunicarea informațiilor respective nu lezează drepturile şi interesele legitime ale altor persoane.

(7) Dacă există îndoieli cu privire la obligativitatea oferirii unei informații, notarul poate cere avizul Camerei Notariale în această privință.

Articolul 11. Obligaţiile notarului

Notarul are următoarele obligaţii:

a) să-şi desfăşoare activitatea în conformitate cu prevederile legale şi cu jurămîntul depus;

b) să acorde persoanelor fizice şi juridice asistenţă notarială, să le explice conţinutul proiectului actului notarial, precum şi drepturile şi obligaţiile lor, să-i avertizeze asupra consecinţelor actelor notariale solicitate;

c) să păstreze secretul profesional care i-a devenit cunoscut în exercitarea activităţii sale, cu excepțiile prevăzute de lege;

d) să încheie un contract de asigurare de răspundere profesională;

e) să asigure condiţii pentru efectuarea stagiului de către notarii stagiari;

f) să țină evidența contabilă şi să achite toate plăţile obligatorii aferente activităţii notariale în condiţiile legii;

g) să păstreze, să ordoneze, să gestioneze şi să transmită arhiva activităţii notariale în condiţiile legii;

g[1]) să preia, în conformitate cu ordinul ministrului justiției, arhiva activității notarului a cărui activitate se suspendă sau încetează;

h) să participe anual la cursuri de instruire cu o durată totală de cel puțin 40 de ore academice;

i) să prezinte rapoartele prevăzute de legislaţie;

j) să ofere organelor de control actele și datele solicitate în limitele controlului efectuat;

k) să îndeplinească alte obligaţii stabilite prin lege şi Codul de etică al

notarilor.

Articolul 19. Răspunderea disciplinară a notarului stagiar

(1) Notarul stagiar răspunde disciplinar pentru abaterile de la obligaţiile ce îi revin potrivit legii.

(2) Constituie abatere disciplinară:

c) divulgarea secretului profesional;

Articolul 24. Comisia de licenţiere

(1) Comisia de licenţiere se formează prin ordinul ministrului justiţiei şi este compusă din 7 membri: 3 membri aleşi de către Adunarea Generală a Notarilor, 4 membri desemnaţi de către Ministerul Justiţiei, dintre care un reprezentant din rîndul societăţii civile selectat prin concurs de către Ministerul Justiţiei. Procedura de selectare prin concurs a membrului Comisiei de licenţiere din rîndul societăţii civile este stabilită în regulamentul aprobat prin ordinul ministrului justiţiei, după consultarea Camerei Notariale. Dacă, în termen de 30 de zile de la solicitarea ministrului justiţiei, Adunarea Generală a Notarilor nu a ales membrii în Comisia de licenţiere, aceştia sînt numiţi de ministrul justiţiei, în rezultatul concursului organizat de către Ministerul Justiţiei.

(2) Ministrul justiţiei poate respinge candidaturile alese de către Adunarea Generală a Notarilor. Refuzul motivat se expediază Consiliului Camerei Notariale în termen de 15 zile de la data la care acestea i-au fost propuse.

(3) În cazul în care Consiliul Camerei Notariale supune votului repetat candidaturile respinse de către ministrul justiţiei şi acestea sînt aprobate din nou cu votul a 2/3 dintre membrii Consiliului, ministrul justiţiei este obligat să le accepte.

(4) Prin ordin al ministrului justiţiei, conform ordinii şi procedurii stabilite la alin. (1), sînt numiţi şi cei 7 membri supleanţi ai Comisiei de licenţiere.

(5) Preşedintele şi vicepreşedintele Comisiei de licenţiere sînt aleşi prin vot secret de către majoritatea membrilor acesteia. În lipsa preşedintelui, funcţiile acestuia sînt exercitate de către vicepreşedinte.

(6) Preşedintele, membrii şi, după caz, membrii supleanţi ai Comisiei de licenţiere beneficiază, pentru fiecare şedinţă la care participă, de o indemnizaţie echivalentă cu a treia parte (1/3) din salariul mediu pe economie, achitată de către Camera Notarială, însă nu mai mult decît pentru 3 şedinţe pe lună.

(7) Secretarul Comisiei de licenţiere este numit prin ordinul ministrului justiţiei din rîndul angajaţilor Ministerului Justiţiei.

(8) Un membru al Comisiei de licenţiere sau un membru supleant al acesteia care lipseşte nemotivat de la 2 şedinţe consecutive este exclus prin ordinul ministrului justiţiei din Comisie şi înlocuit cu un alt membru supleant.

(9) Secretariatul Comisiei de licenţiere va fi asigurat de Ministerul Justiţiei.

(10) Regulamentul de organizare şi funcţionare a Comisiei de licenţiere se aprobă prin ordinul ministrului justiţiei după consultarea Camerei Notariale.

Articolul 25. Modul de luare a deciziilor

(5) Membrii Comisiei de licenţiere sînt obligaţi să păstreze secretul profesional şi să nu divulge informaţia cunoscută în exercitarea calităţii de membru.

PARLAMENTUL

LEGEA Nr. 246 din 15-11-2018

privind procedura notarială

Publicat : 01-02-2019 în Monitorul Oficial Nr. 30-37 art. 89

Articolul 1. Domeniul de reglementare

(1) Prezenta lege stabileşte principiile procedurii notariale, competenţa notarului, procedura de întocmire a actelor notariale şi de îndeplinire a acţiunilor notariale, cerinţele înaintate faţă de acestea.

(2) Prevederile prezentei legi se aplică notarilor şi altor persoane abilitate prin lege cu atribuţii de autentificare a actelor juridice și legalizare a copiilor, extraselor și semnăturilor de pe documente.

Articolul 2. Principiile procedurii notariale

Procedura notarială este guvernată de următoarele principii:

a) legalitatea;

b) independenţa notarului şi supunerea numai legii;

c) întocmirea actelor notariale în mod egal pentru toate persoanele, fără discriminare;

d) imparţialitatea;

e) confidenţialitatea;

f) caracterul nelitigios al procedurii notariale.

Articolul 3. Asigurarea confidenţialităţii

(1) Notarul creează în cadrul biroului notarului condiţiile necesare pentru asigurarea confidenţialităţii. Dacă actul notarial este întocmit în afara sediului biroului notarului, solicitantul actului notarial este obligat să asigure crearea condiţiilor necesare pentru păstrarea confidenţialităţii.

(2) Notarul, notarul stagiar şi personalul care asigură activitatea notarului au obligaţia să păstreze secretul profesional cu privire la actele şi faptele despre care au luat cunoştinţă în cadrul activităţii lor, chiar şi după încetarea funcţiei, respectiv după încetarea raporturilor de muncă, cu excepţia cazurilor în care legea, persoanele care au oferit informaţiile, după caz, subiecţii datelor cu caracter personal sau instanţa de judecată îl eliberează de această obligaţie.

(3) Terţele persoane pot asista la întocmirea actului notarial dacă solicitantul actului notarial a solicitat prin cerere acest fapt. În acest caz, notarul va stabili identitatea terţilor care asistă la întocmirea actului şi va cere acestora depunerea declaraţiei de confidenţialitate.

(4) Modelul declaraţiei de confidenţialitate este aprobat de către Camera Notarială.

PARLAMENTUL

LEGEA Nr. 271 din 15-12-2017

privind auditul situațiilor financiare

Publicat : 12-01-2018 în Monitorul Oficial Nr. 7-17 art. 48

Versiune in vigoare din 01.01.19 in baza modificărilor prin LP234 din 08.11.18, MO448-460/07.12.18 art.733;

Articolul 1. Obiectul de reglementare

Prezenta lege stabilește cadrul juridic privind organizarea auditului de către entitățile de audit, reglementează exercitarea profesiei de auditor, supravegherea auditului, precum și cerințele specifice auditului entităților de interes public.

Articolul 2. Noțiuni

(1) În sensul prezentei legi, se definesc următoarele noțiuni:

audit – auditul situațiilor financiare individuale sau al situațiilor financiare consolidate în măsura în care:

a) este obligatoriu conform prevederilor legislației;

b) este efectuat la solicitarea acționarilor (asociaților) entităților auditate;

auditor – persoană fizică care deține certificat de calificare al auditorului și care este înregistrată în conformitate cu prevederile prezentei legi;

certificat de calificare al auditorului – document, eliberat în modul stabilit de prezenta lege, ce confirmă calificarea profesională de auditor;

Codul etic al profesioniştilor contabili – cerinţe de etică, emise pentru profesioniștii contabili de către Consiliul pentru Standarde Internaţionale de Etică pentru Contabili, acceptate pentru a fi aplicate pe teritoriul Republicii Moldova (în continuare – *Cod etic*);

entitate de audit – entitate constituită în conformitate cu legislația civilă și înregistrată în conformitate cu prevederile prezentei legi;

nepractician – orice persoană fizică care, pe durata activității în cadrul Consiliului de supraveghere publică a auditului (în continuare – Consiliu) și pe parcursul a cel puțin 3 ani precedenți, nu a efectuat audit, nu a deținut acțiuni (părți sociale) în capitalul social al unei entități de audit, nu a fost membru al consiliului, al organului executiv sau de supraveghere a unei entități de audit și nu a fost angajată la o entitate de audit;

risc de audit – riscul exprimării de către auditor a unei opinii de audit necorespunzătoare în cazul în care situaţiile financiare conțin denaturări semnificative;

standarde de audit – standarde internaționale de audit, emise de către Consiliul pentru Standarde Internaţionale de Audit și Asigurare, care se aplică pentru efectuarea auditului, acceptate pentru a fi aplicate pe teritoriul

Republicii Moldova;

standarde de control al calităţii – standarde internaţionale de control al calităţii, emise de către Consiliul pentru Standarde Internaţionale de Audit şi Asigurare, care se aplică pentru controlul intern al calităţii, acceptate pentru a fi aplicate pe teritoriul Republicii Moldova;

standarde conexe – standarde internaţionale pentru misiuni de revizuire, de asigurare şi pentru servicii conexe, emise de către Consiliul pentru Standarde Internaţionale de Audit şi Asigurare, acceptate pentru a fi aplicate pe teritoriul Republicii Moldova.

Articolul 20. Etica profesională

(1) Principiile de etică profesională sînt următoarele:

a) integritate;

b) obiectivitate;

c) competenţă profesională şi atenţia cuvenită;

d) confidenţialitate;

e) comportamentul profesional.

(2) Principiile de etică profesională se aplică conform Codului etic.

(3) Auditorul face uz de scepticismul profesional în procesul efectuării auditului, inclusiv la evaluarea estimărilor privind valorile juste, la verificarea deprecierilor activelor, a provizioanelor şi a fluxurilor de numerar viitoare relevante pentru continuitatea activităţii entităţii auditate.

Articolul 22. Confidenţialitatea şi secretul profesional

(1) Auditorul și entitatea de audit respectă confidenţialitatea și secretul profesional privind informaţiile referitoare la activitatea entităţii auditate, obţinute în timpul exercitării auditului. Obligaţia de a respecta confidenţialitatea şi secretul profesional rămîne în vigoare şi după încetarea contractului de audit.

(2) Auditorul și entitatea de audit asigură respectarea confidenţialităţii și a secretului profesional și din partea personalului care îşi desfăşoară activitatea sub controlul său, precum şi din partea persoanelor care oferă consultanţă şi asistenţă.

(3) Nu se consideră încălcare a principiului confidențialității și a secretului profesional prezentarea informațiilor:

a) la solicitarea instanței judecătorești și a organului de urmărire penală;

b) în cazul efectuării controlului extern al calității de către Consiliu;

c) în cazul în care prezentarea informațiilor este autorizată de către entitatea auditată;

d) în alte cazuri prevăzute de legislație.

PARLAMENTUL

L E G EA nr. 202 din 06.10.2017

privind activitatea băncilor

Monitorul Oficial al R. Moldova nr. 434-439 art. 727 din 15.12.2017

Articolul 3. Definiţii

bancă – persoană juridică a cărei activitate constă în atragerea de depozite sau de alte fonduri rambursabile de la public şi în acordarea de credite în cont propriu;

Capitolul 6

CERINŢE DE PUBLICARE PENTRU BĂNCI

Articolul 91. Sfera de aplicare a cerinţelor de publicare

(1) În scopul asigurării disciplinei şi transparenţei pieţei, băncile trebuie să facă publice informaţii referitoare cel puţin la cadrul de administrare a activităţii, fondurile proprii, cerinţele de capital, lichiditate, expunerile la risc, amortizoarele de capital, alţi indicatori-cheie, politicile interne, inclusiv politica de remunerare, în măsura şi condiţiile prevăzute în actele normative emise în aplicarea prezentei legi.

(2) Aprobarea acordată de Banca Naţională a Moldovei în temeiul art.70 alin.(2) face obiectul publicării de către bănci a informaţiilor prevăzute în actele normative ale Băncii Naţionale a Moldovei, aferente riscului operaţional.

(3) Băncile trebuie să publice separat pe fiecare stat în care a înfiinţat o sucursală informaţiile agregate prevăzute în actele normative ale Băncii Naţionale a Moldovei. Informaţiile respective sînt supuse auditului în conformitate cu art.85 şi sînt publicate ca anexă la propriile situaţii financiare anuale individuale şi consolidate ale băncii respective.

(4) Băncile trebuie să adopte politici formale pentru asigurarea respectării cerinţelor de publicare stabilite şi pentru evaluarea adecvării datelor şi informaţiilor publicate.

(5) Băncile trebuie să furnizeze, la cererea persoanelor care solicită un credit, o explicaţie în scris cu privire la încadrarea lor într-un anumit rating.

(6) Băncile, prin intermediul paginilor web, trebuie să explice modul în care pun în aplicare cerinţele prevăzute la art.39 alin.(1) şi art.40–44.

(7) Prevederile prezentului capitol nu aduc atingere normelor legale prevăzute în alte legi aferente publicării informaţiei.

Articolul 92. Frecvenţa de publicare

(1) Băncile trebuie să facă publice datele şi informaţiile prevăzute la art.91, cel puţin anual, imediat ce acestea sînt disponibile şi nu mai tîrziu de data la care sînt publicate situaţiile financiare anuale.

(2) Băncile evaluează necesitatea publicării datelor şi informaţiilor prevăzute la art.91 cu o frecvenţă mai mare prin luarea în considerare a criteriilor relevante ale activităţii desfăşurate, prevăzute în actele normative emise în aplicarea prezentei legi.

Articolul 93. Mijloace de publicare

(1) Băncile pot stabili mijloacele de informare în masă, locaţia şi mijloacele de verificare adecvate pentru a respecta efectiv cerinţele de publicare prevăzute în prezenta lege. În măsura în care este posibil, băncile trebuie să asigure utilizarea aceloraşi mijloace sau a aceleiaşi locaţii pentru publicarea tuturor datelor şi informaţiilor.

(2) Prezentările echivalente de date şi informaţii către piaţă, realizate de bancă în baza cerinţelor privind publicarea situaţiilor financiare, a informaţiilor privind activitatea băncii pe o piaţă reglementată sau a altor asemenea cerinţe, pot fi considerate că asigură respectarea cerinţelor de publicare potrivit prezentei legi. Dacă datele şi informaţiile nu sînt incluse în situaţiile financiare, băncile trebuie să indice unde pot fi găsite.

Articolul 94. Cerinţe specifice de publicare

(1) Banca Naţională a Moldovei poate impune unei bănci:

a) publicarea informaţiilor menţionate la art.91 alin.(1) cu o frecvenţă mai ridicată decît cea anuală şi stabilirea termenelor de publicare;

b) utilizarea unor modalităţi şi forme de publicare specifice, altele decît situaţiile financiare.

(2) Banca Naţională a Moldovei poate impune întreprinderilor-mamă să publice anual, fie integral, fie prin trimiteri la informaţii echivalente, o descriere a structurii juridice, precum şi de guvernanţă, şi organizatorice a grupului de bănci şi/sau societăţi de investiţii, incluzînd informaţii privind entităţile între care există legături strînse, precum şi în ceea ce priveşte cadrul de administrare a activităţii.

Titlul IV

POLITICI DE PREVENIRE ŞI COMBATERE A SPĂLĂRII BANILOR ŞI FINANŢĂRII TERORISMULUI. SECRETUL BANCAR ŞI CONFLICTELE DE INTERESE

Articolul 95. Politici de prevenire şi combatere a spălării banilor şi finanţării terorismului

(1) Banca trebuie să dispună de politici şi proceduri interne în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului şi trebuie să aplice cerinţele legislaţiei cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului.

(2) Banca nu poate ascunde, converti sau transfera bani sau alte valori, ştiind că acestea provin din activităţi criminale, pentru mascarea originii lor ilegale, şi nici asista persoana angajată în astfel de activităţi pentru evitarea consecinţelor legale ale faptelor ei.

Articolul 96. Obligativitatea păstrării confidenţialităţii

(1) Banca este obligată să păstreze confidenţialitatea asupra tuturor faptelor, datelor şi informaţiilor referitoare la activitatea sa, precum şi asupra oricăror fapte, date sau informaţii, aflate la dispoziţia sa, referitoare la persoana, bunurile, activitatea, afacerea, relaţiile personale sau de afaceri ale clienţilor băncii ori informaţiile referitoare la conturile clienţilor (solduri, rulaje, operaţiuni derulate), tranzacţiile încheiate de clienţi, precum şi a altor informaţii despre clienţi care i-au devenit cunoscute.

(2) În sensul prezentului capitol, informaţiile prevăzute la alin.(1) constituie secret bancar.

(3) Membrii organului de conducere şi funcţionarii băncii, persoanele care acţionează în numele băncii şi alte persoane care, în virtutea executării obligaţiilor de serviciu, au obţinut acces la informaţia prevăzută la alin.(1) au obligaţia de a păstra secretul bancar, de a nu folosi informaţia indicată în alte scopuri decît cele de serviciu. Această obligaţie continuă să existe şi după încetarea activităţii persoanelor menţionate mai sus sau în perioada suspendării activităţii lor.

(4) Se interzice furnizarea de către bancă a informaţiei referitoare la clienţii altei bănci, chiar dacă numele/denumirea acestora sînt indicate în documentele şi contractele clientului sau figurează în cadrul operaţiunilor acestuia.

(5) Banca îşi organizează activitatea astfel încît membrii organului de conducere, funcţionarii şi persoanele care acţionează în numele ei să nu fie puşi în situaţia cînd obligaţiile lor faţă de un client intră în conflict cu obligaţiile faţă de un alt client sau cînd interesele lor proprii intră în conflict cu obligaţiile faţă

de un client.

Articolul 97. Condiţiile furnizării informaţiei ce constituie secret bancar

(1) Obligaţia de păstrare a secretului bancar nu poate fi opusă unei autorităţi competente în exercitarea atribuţiilor sale de supraveghere pe bază individuală şi/sau consolidată.

(2) Furnizarea informaţiei care constituie secret bancar, inclusiv către autorităţile publice abilitate prin legi speciale să solicite informaţii de la persoanele fizice şi juridice, se efectuează în strictă conformitate cu prezentul articol.

(3) Informaţia care constituie secret bancar urmează a fi furnizată de bancă, în măsura în care furnizarea acestei informaţii este justificată de scopul pentru care este solicitată, în următoarele cazuri:

a) la solicitarea clientului băncii sau a reprezentantului acestuia;

b) în cazul decesului clientului băncii, la solicitarea moştenitorului acestuia, cu anexarea certificatului de moştenitor, precum şi la solicitarea notarului care a deschis procedura succesorală, cu anexarea copiei certificatului de deces al clientului băncii;

c) la solicitarea organului de urmărire penală, cu autorizaţia judecătorului de instrucţie, privind cauza penală concretă;

d) la solicitarea instanţei de judecată, în scopul soluţionării unei cauze aflate pe rol;

e) la solicitarea scrisă a altor autorităţi publice ori din oficiu, dacă prin lege specială aceste autorităţi publice au dreptul, în scopul îndeplinirii atribuţiilor lor specifice, să solicite şi/sau să primească astfel de informaţii de la bancă;

f) la solicitarea Ministerului Finanţelor, în conformitate cu Legea nr.419/2006 cu privire la datoria sectorului public, garanţiile de stat şi recreditarea de stat, a informaţiei privind împrumuturile acordate întreprinderilor de stat/municipale, societăţilor comerciale cu capital integral sau majoritar public şi unităţilor administrativ-teritoriale, necesară pentru monitorizarea sectorului public;

g) la solicitarea executorului judecătoresc, în temeiul şi în limitele prevăzute de documentul executoriu;

h) cînd banca justifică un interes legitim.

(4) Solicitarea de furnizare a informaţiei ce constituie secret bancar, înaintată de autorităţile menţionate la alin.(3), trebuie să conţină temeiul legal al solicitării, datele de identitate ale persoanei la care se referă informaţia confidenţială solicitată, categoria informaţiei solicitate şi scopul pentru care se solicită aceasta. Solicitarea înaintată trebuie să fie semnată de persoana cu funcţie de răspundere împuternicită şi să aibă aplicată ştampila autorităţii date. Solicitarea informaţiei, înaintată de organul fiscal al Republicii Moldova, poate să

nu conţină datele de identitate ale persoanei (persoanelor) la care se referă informaţia solicitată în cazurile şi/sau în condiţiile Acordului de cooperare dintre Guvernul Republicii Moldova şi Guvernul Statelor Unite ale Americii pentru facilitarea implementării prevederilor Actului privind îndeplinirea obligaţiilor fiscale cu privire la conturile străine (FATCA).

(5) Nu constituie încălcare a obligaţiei de păstrare a secretului bancar:

a) furnizarea către Banca Naţională a Moldovei a informaţiei necesare exercitării atribuţiilor ei;

b) furnizarea informaţiei şi a datelor întocmite astfel încît identitatea şi informaţiile privind activitatea fiecărui client al băncii nu pot fi identificate;

c) furnizarea obligatorie organelor fiscale a informaţiei privind deschiderea, modificarea şi închiderea conturilor bancare, în cazurile şi cu referinţă la categoriile de contribuabili prevăzute de lege;

d) furnizarea informaţiei societăţii de audit a băncii, în limitele necesare exercitării de către aceasta a activităţii de audit;

e) furnizarea informaţiei Fondului de garantare a depozitelor în sistemul bancar, în limitele necesare exercitării atribuţiilor acestuia;

f) furnizarea informaţiei birourilor istoriilor de credit referitoare la creditele acordate, în conformitate cu legea specială;

g) furnizarea informaţiei Serviciului prevenirea şi combaterea spălării banilor despre orice activitate sau tranzacţie suspectă, în conformitate cu legislaţia cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului;

h) furnizarea informaţiei entităţilor ce aparţin grupului din care face parte banca, necesară pentru organizarea supravegherii pe bază consolidată şi pentru combaterea spălării banilor şi finanţării terorismului;

i) furnizarea lunară către Ministerul Finanţelor a informaţiei privind încasările, plăţile şi soldurile de mijloace băneşti în conturile deschise în bănci de către instituţiile publice finanţate de la bugetul public naţional;

j) furnizarea de informaţii la solicitarea Ministerului Finanţelor în scopul exercitării atribuţiilor pentru conturile deschise în bănci de către instituţiile publice finanţate de la bugetul public naţional;

k) furnizarea informaţiei în conformitate cu prevederile şi în limitele Acordului de cooperare dintre Guvernul Republicii Moldova şi Guvernul Statelor Unite ale Americii pentru facilitarea implementării prevederilor Actului privind îndeplinirea obligaţiilor fiscale cu privire la conturile străine (FATCA).

(6) Persoanele şi organele abilitate să solicite şi să primească informaţiile ce constituie secret bancar sînt obligate să păstreze confidenţialitatea acestora şi

le pot utiliza numai în scopul pentru care le-au solicitat sau le-au fost furnizate, potrivit legii, şi sînt obligate să nu le furnizeze sau să le divulge persoanelor terţe, cu excepţia cazurilor de executare a obligaţiilor prevăzute de lege.

[Art.97 modificat prin Legea nr.160 din 26.07.2018, în vigoare 17.09.2018]

Articolul 98. Declararea interesului material

(1) Orice membru al organului de conducere sau persoană care deţine o funcţie-cheie în banca care este parte într-un contract efectiv sau într-un contract propus băncii privind interese materiale sau care este conducător al unei persoane parte într-un contract material efectiv sau propus băncii sau care are un interes material faţă de această persoană trebuie să dezvăluie în scris băncii interesul său material în momentul în care ia cunoştinţă sau ar fi trebuit să ia cunoştinţă de existenţa unui astfel de contract.

(2) Orice membru al organului de conducere sau persoană care deţine o funcţie-cheie este obligată să prezinte consiliului băncii, cel puţin o dată pe an, o notă scrisă, în care să dezvăluie suficient conflictul de interese. Se consideră dezvăluire suficientă a conflictului de interese indicarea numelui şi adresei asociaţilor persoanelor respective, detaliilor esenţiale despre activităţile lor, intereselor de familie care confirmă că aceştia au interese materiale în contractele încheiate cu orice persoană numită în notă.

(3) Orice membru al organului de conducere sau persoană ce deţine o funcţie-cheie care are interes material într-un contract trebuie să părăsească orice şedinţă la care este pus în discuţie acest contract. Totodată, prezenţa persoanelor respective la şedinţă se ia în calcul la stabilirea cvorumului, iar la votare se consideră că acestea s-au abţinut. În caz de paritate a voturilor, cel al preşedintelui şedinţei se consideră hotărîtor.

(4) În aplicarea prevederilor alin.(1) şi (2), interesul material şi conflictul de interese se determină în conformitate cu prevederile art.85 şi 86 din Legea nr.1134/1997 privind societăţile pe acţiuni.

(5) Dacă persoanele menţionate la alin.(1) nu şi-au dezvăluit conflictul de interese:

a) judecătoria poate, la cererea băncii, a unuia sau mai multor acţionari ai acesteia sau a Băncii Naţionale a Moldovei, să suspende contractul pe un termen stabilit de prima;

b) Banca Naţională a Moldovei poate dispune băncii măsurile de supraveghere prevăzute de art.139 şi/sau aplica sancţiunile prevăzute la art.141.

(6) Independent de obligaţiile enumerate la art.96 alin.(5), membrul organului de conducere sau persoana care deţine funcţie-cheie în cadrul băncii are obligaţia faţă de banca în care îşi desfăşoară activitatea şi faţă de clienţii băncii de a pune interesele băncii şi ale clienţilor mai presus de interesul pecuniar propriu.

Capitolul 3

SCHIMBUL DE INFORMAŢII CU ALTE AUTORITĂŢI COMPETENTE ŞI ASIGURAREA CONFIDENŢIALITĂŢII ÎN PROCESUL DE EXERCITARE A ATRIBUŢIILOR DE SUPRAVEGHERE

Articolul 126. Secretul profesional al Băncii Naţionale a Moldovei

(1) Membrii organelor de conducere şi salariaţii Băncii Naţionale a Moldovei, precum şi salariaţii societăţilor de audit sau experţii numiţi de Banca Naţională a Moldovei pentru efectuarea de verificări la sediul băncilor, potrivit prevederilor art.106 alin.(5), sînt obligaţi să păstreze secretul profesional asupra oricărei informaţii confidenţiale de care iau cunoştinţă în cursul exercitării atribuţiilor lor în aplicarea prezentei legi. Membrii organelor de conducere şi salariaţii Băncii Naţionale a Moldovei sînt obligaţi să păstreze secretul profesional şi după încetarea activităţii în cadrul băncii.

(2) Persoanele prevăzute la alin.(1) nu pot divulga informaţii confidenţiale niciunei persoane sau autorităţi, cu excepţia furnizării acestor informaţii în formă sumară sau agregată, astfel încît banca să nu poată fi identificată.

(3) Dacă o bancă a fost sau este supusă lichidării silite, informaţiile confidenţiale care nu se referă la terţii implicaţi în acţiuni legate de lichidarea băncii pot fi divulgate în cadrul procedurilor civile.

(4) Publicarea de către Banca Naţională a Moldovei a rezultatelor simulărilor de criză în conformitate cu art.100 alin.(5) nu constituie încălcare a obligaţiei menţionate la alin.(1).

(5) Dispoziţiile alin.(1)–(3) nu aduc în niciun fel atingere prevederilor legislaţiei potrivit cărora se poate impune divulgarea de informaţii confidenţiale în anumite situaţii.

(6) În sensul prezentului capitol, informaţiile confidenţiale înseamnă orice informaţii ce reprezintă secret bancar, comercial, fiscal şi alt secret ocrotit de lege, precum şi informaţiile create de către Banca Naţională a Moldovei în scopul ori în legătură cu exercitarea atribuţiilor ei, a căror divulgare ar putea dăuna interesului sau prestigiului persoanei la care se referă.

(7) Prevederile art.8 alin.(2) lit.b) din Legea nr.548/1995 cu privire la Banca Naţională a Moldovei nu sînt aplicabile în cazul în care la şedinţa Consiliului de supraveghere sau a Comitetului executiv al Băncii Naţionale a Moldovei se discută chestiuni legate de supravegherea prudenţială a băncilor.

Articolul 127. Utilizarea informaţiilor confidenţiale

(1) Prin derogare de la art.36 din Legea nr.548/1995, Banca Naţională a Moldovei poate utiliza informaţiile primite potrivit art.126 doar în exercitarea atribuţiilor sale de supraveghere a băncilor şi numai în următoarele situaţii:

a) examinarea îndeplinirii condiţiilor de licenţiere a băncilor, precum şi facilitarea supravegherii, pe bază individuală şi/sau consolidată, a condiţiilor de desfăşurare a activităţii băncilor, în special cu privire la lichiditate, solvabilitate, expunerile mari, procedurile administrative şi contabile şi la mecanismele de control intern;

b) aplicarea de sancţiuni;

c) contestarea actelor emise de Banca Naţională a Moldovei;

d) în cadrul unor proceduri judiciare iniţiate împotriva unei decizii a Băncii Naţionale a Moldovei sau a prevederilor altor legi aplicabile băncilor.

(2) Prevederile art.36 din Legea nr.548/1995 cu privire la Banca Naţională a Moldovei nu se aplică în cazul schimbului de informaţii şi al obligaţiei de păstrare a secretului profesional în exercitarea competenţelor de supraveghere prudenţială, potrivit prezentei legi, de către Banca Naţională a Moldovei.

Articolul 128. Acorduri de cooperare

(1) Banca Naţională a Moldovei poate încheia acorduri de cooperare referitoare la schimbul de informaţii cu autorităţile competente din alte state sau cu alte autorităţi ori organisme din alte state prevăzute la art.129 şi art.130, în condiţiile în care informaţiile furnizate sînt supuse unor cerinţe de păstrare a secretului profesional cel puţin echivalente celor prevăzute la art.126. Schimbul de informaţii trebuie să fie circumscris scopului îndeplinirii atribuţiilor de supraveghere ale autorităţilor sau organismelor menţionate.

(2) În cazul în care informaţiile primite de Banca Naţională a Moldovei provin dintr-un alt stat, acestea se divulgă doar cu acordul expres al autorităţilor care le-au transmis, iar în unele cazuri, doar în scopurile pentru care autorităţile în cauză şi-au dat acordul.

Articolul 129. Schimbul de informaţii între autorităţi competente

(1) În exercitarea atribuţiilor de supraveghere, prevederile art.126 şi 127 nu împiedică schimbul de informaţii dintre Banca Naţională a Moldovei şi autorităţile competente din Republica Moldova ori din alte state sau dintre Banca Naţională a Moldovei şi următoarele entităţi din Republica Moldova sau din alte state:

a) autorităţile responsabile cu supravegherea altor entităţi din sectorul financiar şi autorităţile responsabile cu supravegherea pieţelor financiare;

b) autorităţile sau organismele responsabile cu menţinerea stabilităţii sistemului financiar, prin utilizarea reglementărilor/instrumentelor macroprudenţiale;

c) organismele sau autorităţile împuternicite să aplice măsuri de salvgardare care au ca scop protejarea stabilităţii sistemului financiar;

d) sistemele de protecţie contractuală sau instituţională care constau într-un acord de stabilire contractuală sau legală a responsabilităţilor care protejează băncile şi le asigură, în special, lichiditatea şi solvabilitatea pentru a evita falimentul, în cazul în care este necesar băncilor;

e) organismele implicate în falimentul şi în lichidarea băncii, precum şi în alte proceduri similare;

f) societăţile de audit ale băncilor, societăţilor de investiţii, asigurătorilor, precum şi ale altor societăţi financiare nonbancare.

(2) În sensul alin.(1) lit.c), măsuri de salvgardare reprezintă măsurile destinate menţinerii sau restabilirii situaţiei financiare a unei bănci şi care ar putea afecta drepturile preexistente ale unor terţi, inclusiv măsurile care implică posibilitatea unei suspendări a plăţilor, a măsurilor de executare sau a unei reduceri a creanţelor; aceste măsuri includ aplicarea instrumentelor de rezoluţie şi exercitarea competenţelor de rezoluţie.

(3) Prevederile art.126 şi 127 nu împiedică furnizarea către organismele care administrează scheme de garantare a depozitelor sau scheme de compensare a investitorilor a informaţiilor necesare exercitării funcţiilor acestora.

(4) Informaţiile primite de autorităţile, organismele şi societăţile de audit din Republica Moldova potrivit prevederilor alin.(1) sînt supuse cerinţelor referitoare la secretul profesional prevăzute la art.126.

(5) Banca Naţională a Moldovei schimbă informaţii cu autorităţile, organismele şi societăţile de audit din alte state, potrivit prevederilor alin.(1), numai dacă informaţiile primite de respectivele autorităţi, organisme sau de societăţi de audit sînt supuse unor cerinţe de păstrare a secretului profesional cel puţin echivalente celor prevăzute la art.126.

Articolul 130. Schimbul de informaţii cu alte autorităţi

(1) Fără a aduce atingere prevederilor art.126–128, Banca Naţională a Moldovei poate schimba informaţii cu autorităţi din Republica Moldova sau din alte state, responsabile cu monitorizarea:

a) organismelor implicate în falimentul şi lichidarea băncilor, precum şi în alte proceduri similare;

b) sistemelor de protecţie contractuală sau instituţională, astfel cum sînt prevăzute la art.129 alin.(1) lit.d);

c) societăţilor de audit ale băncilor, societăţilor de investiţii, asigurătorilor, precum şi ale altor societăţi financiare nonbancare.

(2) Schimbul de informaţii prevăzut la alin.(1) se realizează cu respectarea următoarelor condiţii:

a) informaţiile trebuie să fie destinate îndeplinirii atribuţiilor de monitorizare prevăzute la alin.(1);

b) informaţiile primite de către autorităţile prevăzute la alin.(1), din Republica Moldova sau din alte state, sînt supuse unor cerinţe de păstrare a secretului profesional, prevăzute de legislaţia naţională, cel puţin echivalente celor prevăzute la art.126;

c) în cazul în care informaţiile provin dintr-un alt stat, acestea nu sînt divulgate fără acordul expres al autorităţii competente care le-a furnizat, iar în unele cazuri, doar în scopurile pentru care autoritatea în cauză şi-a dat acordul.

(3) Fără a aduce atingere prevederilor art.126–128, cu scopul de a consolida stabilitatea şi integritatea sistemului financiar, Banca Naţională a Moldovei poate schimba informaţii cu autorităţi sau organisme din Republica Moldova sau din alte state responsabile, în temeiul legii, de depistarea şi investigarea încălcărilor legislaţiei privind societăţile pe acţiuni şi/sau privind prevenirea şi combaterea spălării banilor şi finanţării terorismului.

(4) Schimbul de informaţii prevăzut la alin.(3) se realizează cu respectarea următoarelor condiţii:

a) informaţiile respective sînt schimbate în scopul îndeplinirii sarcinilor de depistare şi investigare a încălcărilor aduse dreptului societăţilor comerciale;

b) informaţiile primite de autorităţile sau organismele, prevăzute la alin.(3), din Republica Moldova sau din alte state sînt supuse unor cerinţe de păstrare a secretului profesional, prevăzute de legislaţia naţională, cel puţin echivalente celor prevăzute la art.126;

c) în cazul în care informaţiile provin dintr-un alt stat, acestea nu sînt divulgate fără acordul expres al autorităţii competente care le-a furnizat, iar în unele cazuri, doar în scopurile pentru care autoritatea în cauză şi-a dat acordul.

(5) Autorităţile sau organismele din Republica Moldova avînd competenţele prevăzute la alin.(3) pot schimba informaţii cu autorităţile competente din alte state, cu respectarea condiţiilor prevăzute la alin.(4), inclusiv în situaţia în care aceste autorităţi sau organisme desfăşoară activitatea de detectare şi investigare cu ajutorul unor persoane anume desemnate în acest scop, care nu sînt funcţionari publici.

(6) Autorităţile sau organismele din Republica Moldova, prevăzute la alin. (3) comunică autorităţilor competente care le furnizează informaţii, numele şi responsabilităţile precis determinate ale persoanelor cărora li se transmit respectivele informaţii.

Articolul 131. Transmiterea de informaţii relevante sub aspect monetar, al protecţiei depozitelor, al riscului sistemic sau al supravegherii plăţilor

(1) Prevederile prezentului capitolul nu împiedică Banca Naţională a Moldovei, în calitate de autoritate competentă, să transmită autorităţilor şi organismelor de mai jos informaţiile destinate îndeplinirii atribuţiilor acestora:

a) băncilor centrale ale altor state şi altor organisme cu funcţii similare, în calitate de autorităţi monetare, dacă aceste informaţii sînt relevante pentru exercitarea atribuţiilor statutare care le revin, inclusiv coordonarea politicii monetare şi furnizarea de lichidităţi, supravegherea sistemelor de plăţi, a sistemelor de clearing şi decontare şi menţinerea stabilităţii sistemului financiar;

b) sistemelor de protecţie contractuală sau instituţională, astfel cum sînt prevăzute la art.129 alin.(1) lit.d);

c) altor autorităţi publice responsabile de supravegherea sistemelor de plăţi, dacă este cazul;

d) autorităţilor responsabile de stabilitatea financiară şi riscul sistemic.

(2) Prevederile prezentului capitol nu împiedică autorităţile sau organismele menţionate la alin.(1) să comunice Băncii Naţionale a Moldovei informaţiile în măsura în care îi sînt necesare în situaţiile prevăzute la art.127.

(3) Informaţiile primite de Banca Naţională a Moldovei în conformitate cu alin.(2) sînt supuse cerinţelor prevăzute la art.126 referitoare la secretul profesional.

(4) Informaţiile furnizate de Banca Naţională a Moldovei în conformitate cu alin.(1) trebuie să fie supuse unor cerinţe de păstrare a secretului profesional, prevăzute de legislaţia naţională, cel puţin echivalente celor de la art.126.

Articolul 132. Transmiterea informaţiilor către alte entităţi

(1) Banca Naţională a Moldovei poate furniza anumite informaţii referitoare la supravegherea prudenţială a băncilor comisiilor de anchetă ale Parlamentului, Curţii de Conturi şi altor instituţii din Republica Moldova cu competenţe de anchetă în următoarele condiţii:

a) aceste instituţii au un mandat legal special de investigare sau examinare a activităţii Băncii Naţionale a Moldovei de supraveghere şi reglementare prudenţială a băncilor;

b) informaţiile sînt necesare strict pentru îndeplinirea mandatului prevăzut la lit.a);

c) persoanele care au acces la informaţii sînt supuse unor cerinţe de păstrare a secretului profesional, prevăzute de legislaţia naţională, cel puţin echivalente celor de la art.126;

d) dacă informaţiile provin de la autorităţi competente şi instituţii dintr-un alt stat, acestea nu se divulgă fără acordul expres al autorităţilor şi instituţiilor respective care le-au transmis, decît în scopurile pentru care respectivele autorităţi şi instituţii şi-au dat acordul.

(2) În măsura în care furnizarea de informaţii potrivit alin.(1) implică prelucrarea de date cu caracter personal, trebuie respectate prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal.

Articolul 133. Divulgarea informaţiilor obţinute prin verificări şi inspecţii

În situaţiile prevăzute la art.132, informaţiile primite de Banca Naţională a Moldovei potrivit art.130 şi cele obţinute ca urmare a verificărilor din cadrul controalelor pe teren sau al inspecţiilor efectuate în condiţiile art.108 nu se divulgă de către aceasta fără acordul expres al autorităţii competente de la care au fost primite informaţiile, respectiv al autorităţii competente din alt stat în care a fost efectuată o astfel de verificare în cadrul controalelor pe teren sau al inspecţiilor.

Articolul 134. Divulgarea informaţiilor privind serviciile de clearing şi decontare

(1) Prevederile prezentului capitol nu împiedică Banca Naţională a Moldovei să furnizeze informaţiile la care se referă prevederile art.126–128 sistemelor de clearing şi decontare sau altor structuri similare constituite, în conformitate cu prevederile legii, în vederea asigurării serviciilor de clearing şi decontare pentru orice piaţă din Republica Moldova, în cazul în care consideră că este necesar să comunice aceste informaţii în scopul asigurării funcţionării corespunzătoare a respectivelor structuri, avînd în vedere riscurile ca participanţii pe piaţă să nu-şi îndeplinească obligaţiile de plată.

(2) Informaţiile primite potrivit prevederilor alin.(1) sînt supuse unor cerinţe referitoare la secretul profesional prevăzute de legislaţia naţională, cel puţin echivalente celor prevăzute la art.126.

(3) În situaţiile prevăzute la alin.(1), informaţiile primite de la alte autorităţi competente conform prezentului capitol nu se divulgă de Banca Naţională a Moldovei fără acordul expres al autorităţii competente care a furnizat informaţiile respective.

Articolul 135. Prelucrarea datelor cu caracter personal

Prelucrarea datelor cu caracter personal în sensul prezentei legi se efectuează în conformitate cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal.

Capitolul 4

CERINŢE DE PUBLICARE PENTRU BANCA NAŢIONALĂ A MOLDOVEI

Articolul 136. Cerinţe generale privind publicarea

(1) Banca Naţională a Moldovei publică următoarele informaţii:

a) textele legilor şi ale actelor normative adoptate în domeniul supravegherii prudenţiale a băncilor, precum şi ale recomandărilor emise în aplicarea acestora;

b) criteriile generale şi metodologiile utilizate pentru analizarea cadrului de administrare a activităţii, strategiilor, proceselor şi mecanismelor implementate de către bănci în vederea respectării dispoziţiilor prezentei legi şi ale actelor normative emise în aplicarea acesteia şi pentru evaluarea riscurilor la care băncile sînt sau pot fi expuse;

c) fără a aduce atingere prevederilor privind secretul profesional, date statistice agregate privind aspectele principale ale aplicării cadrului legal şi de reglementare în domeniul prudenţial, inclusiv numărul şi natura măsurilor de supraveghere conform art.139 alin.(1) lit.a) dispuse faţă de băncile care nu îndeplinesc cerinţele prezentei legi şi ale actelor normative emise în aplicarea acesteia, precum şi ale sancţiunilor şi măsurilor sancţionatoare aplicate conform prevederilor art.141;

d) lista persoanelor care exercită funcţii de conducere în bănci şi în sucursalele băncilor străine.

(2) Informaţiile menţionate la alin.(1) se publică şi sînt accesibile pe pagina web oficială a Băncii Naţionale a Moldovei şi se actualizează periodic.

Articolul 137. Cerinţe de publicare specifice

Banca Naţională a Moldovei publică următoarele informaţii în ceea ce priveşte tratamentul expunerilor la riscul de credit transferat prevăzut de actele normative emise în aplicarea prezentei legi:

a) criteriile generale şi metodologiile adoptate pentru a verifica respectarea cerinţelor stabilite prin actele normative respective;

b) fără a aduce atingere prevederilor privind secretul profesional, o descriere succintă a rezultatului verificărilor prudenţiale şi o descriere a măsurilor aplicate în cazurile de nerespectare de către bănci a cerinţelor prevăzute la lit.a).

PARLAMENTUL
LEGEA Nr. 113 din 17-06-2010
privind executorii judecătoreşti*

Publicat : 06-01-2017 în Monitorul Oficial Nr. 2-8 art. 01

Versiune în vigoare din 30.12.18 în baza modificărilor prin LP238 din 08.11.18, MO441-447 din 30.11.18 art.709

Articolul 1. Domeniul de reglementare

(1) Prezenta lege stabileşte statutul, sarcinile şi responsabilităţile executorilor judecătoreşti, modul de organizare profesională şi de autoadministrare, relaţiile lor cu autorităţile publice, cu organizaţii publice sau private.

(2) Sub incidenţa prezentei legi se află executorii judecătoreşti care efectuează acţiuni procedurale pentru executarea documentelor executorii în conformitate cu dispoziţiile Codului de executare, ale Codului de procedură civilă şi ale altor acte legislative şi normative, autorităţile publice şi organizaţiile implicate în activitatea executorului judecătoresc.

Articolul 2. Activitatea executorului judecătoresc

(1) Executorul judecătoresc este persoană fizică învestită de stat cu competenţa de a îndeplini activităţi de interes public prevăzute de prezenta lege şi de alte legi. În exercitarea atribuţiilor de serviciu, executorul judecătoresc este exponentul puterii de stat. Doar executorul judecătoresc licenţiat şi învestit în condiţiile prezentei legi poate efectua executarea silită.

(2) Activitatea executorului judecătoresc nu este activitate de întreprinzător.

(3) Activitatea executorului judecătoresc se desfăşoară în condiţiile legii, cu respectarea drepturilor şi a intereselor legitime ale părţilor în procedura de executare şi ale altor persoane interesate, fără deosebire de rasă, de naţionalitate, de origine etnică, de limbă, de religie, de sex, de apartenenţă politică, de avere, de origine socială sau de orice alt criteriu.

(4) Executorul judecătoresc nu poate refuza executarea unui act dat în competenţa sa, decît în cazurile şi în condiţiile stabilite de lege.

Articolul 23. Procedura disciplinară

(1) În termen de cel mult 30 de zile de la înregistrarea sesizării privind

tragerea la răspundere disciplinară a executorului judecătoresc va fi numită data examinării ei, care va fi comunicată autorului sesizării, executorului judecătoresc şi membrilor Colegiului disciplinar. În acelaşi termen, copia de pe sesizare este remisă executorului judecătoresc prin una dintre modalitățile stabilite de Consiliul Uniunii Naționale a Executorilor Judecătorești sau prin orice mijloc ce permite confirmarea recepționării. (3) Şedinţele Colegiului disciplinar sînt publice, cu excepţia cazurilor în care Colegiul disciplinar decide, din oficiu sau în baza cererii scrise a executorului judecătoresc ori a autorului sesizării, examinarea cauzei în şedinţă închisă pentru a preveni divulgarea unor informaţii confidenţiale din cadrul procedurii de executare sau pentru protecţia vieţii private.

Articolul 32. Personalul auxiliar al biroului executorului judecătoresc

(1) Pentru asigurarea funcţionării biroului şi activităţilor efectuate de executorul judecătoresc pot fi atraşi specialişti şi lucrători auxiliari.

(2) Persoanele atrase în activităţile biroului executorului judecătoresc sînt obligate să asigure confidenţialitatea datelor ce ţin de procedura de executare, de care au luat cunoştinţă. Divulgarea informaţiei confidenţiale atrage răspundere în condiţiile legii.

PARLAMENTUL

LEGEA Nr. 283 din 04-07-2003

privind activitatea particulară de detectiv şi de pază

Publicat : 19-09-2003 în Monitorul Oficial Nr. 200-203 art. 769

Versiune in vigoare din 12.01.19 in baza modificărilor prin LP245 din 15.11.18 MO 462-466 din 12.12.18 art. 774

Articolul 1. Obiectul reglementării

Prezenta lege stabileşte principiile, scopurile, subiectele şi modul de prestare a serviciilor particulare de investigare şi de pază persoanelor fizice şi juridice, inclusiv celor străine, în condiţiile legii.

Articolul 2. Obiectivele legii

Principalele obiective ale prezentei legi sînt:

a) reglementarea procesului organizatoric de acordare, în bază de contract, a serviciilor particulare de pază de către persoane autorizate în modul stabilit şi a serviciilor particulare de investigare;

b) asigurarea respectării drepturilor şi intereselor legitime ale clienţilor;

c) asigurarea protecţiei sociale a lucrătorilor din organizaţiile de detectiv şi de pază;

d) contribuirea la respectarea intereselor statului şi la menţinerea ordinii publice;

e) asigurarea controlului de stat asupra modului de desfăşurare a serviciilor particulare de investigare şi de pază;

f) prevenirea şi combaterea fenomenului infracţional în organizaţiile de detectiv şi de pază.

Articolul 3. Noţiuni principale

În sensul prezentei legi, se definesc următoarele noţiuni principale:

activitate particulară de detectiv – gen de activitate care constă în acordarea serviciilor de investigare, desfăşurat de către persoane specializate în domeniu, în bază de contract, conform condiţiilor prevăzute de prezenta lege;

activitate particulară de pază – gen de activitate autorizat de acordare a serviciilor de pază întru apărarea vieţii, sănătăţii şi bunurilor de către persoane specializate în domeniu, în bază de contract, conform condiţiilor de autorizare;

subdiviziune specializată de pază – subunitate interioară de pază care nu dispune de statut de persoană juridică, înfiinţată de o persoană juridică sau

de un întreprinzător individual pentru asigurarea securităţii vieţii şi sănătăţii lucrătorilor şi bunurilor sale;

gardian (paznic) – persoană care a absolvit cursuri de pregătire specială pentru a activa în calitate de paznic, a susţinut prin examen dreptul de păstrare şi de port-armă de serviciu şi de mijloace speciale, încadrată în bază de contract în serviciu într-o organizaţie de pază;

gardian (paznic) particular – persoană autorizată pentru a desfăşura activitate de întreprinzător în acordarea de servicii pentru asigurarea securităţii vieţii, sănătăţii şi bunurilor împotriva unor atentate criminale;

sistem de alarmare – ansamblu de instalaţii electronice aferente construcţiilor, compus din centrală de comandă şi de semnalizare optică şi acustică, centrală de comandă şi de semnalizare optică şi acustică împotriva incendiilor, detectoare de prezenţă, detectoare antişoc şi acustice, detectoare de fum, de temperatură, de foc şi de gaze, butoane şi pedale de panică, control acces şi televiziune cu circuit închis, cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor, de natură să asigure o protecţie corespunzătoare obiectivelor şi persoanelor fizice;

operator (supraveghetor) – persoană care supraveghează funcţionarea dispeceratului centralizat de pază şi întruneşte condiţiile de gardian;

grupă mobilă – grup format din 2 sau 3 angajaţi ai organizaţiilor particulare de pază, dotat cu automobil şi mijloace speciale, destinat intervenţiei rapide la primirea semnalelor de alarmă;

proiect al sistemului de alarmare – set de documente care cuprinde calcule tehnice, desene, instrucţiuni etc., necesare pentru instalare şi orice modificare a sistemului de alarmare;

dispecerat de pază centralizat – punct de control destinat pazei centralizate a unor obiective dispersate împotriva pătrunderii nesancţionate sau împotriva incendiilor, cu utilizarea sistemelor de transmitere a înştiinţărilor referitoare la evenimentele ce au loc la obiectivele păzite.

Articolul 4. Principiile activităţii particulare de detectiv şi de pază

(1) Activitatea particulară de detectiv şi de pază se întemeiază pe principiile legalităţii, umanismului, echităţii sociale, respectării drepturilor şi libertăţilor persoanei şi se desfăşoară în interacţiune cu autorităţile publice şi asociaţiile obşteşti în vederea asigurării ordinii de drept.

(2) Activitatea particulară de detectiv şi de pază se desfăşoară în conformitate cu legislaţia.

Articolul 5. Autorizarea şi restricţia activităţii particulare de detectiv şi de pază

(1) Activitatea particulară de detectiv se desfăşoară în condiţiile prezentei legi, cu sau fără notificarea organului de specialitate al Ministerului Afacerilor Interne.

(1^1) Activitatea particulară de pază se desfăşoară în bază de autorizaţie, eliberată de organul de specialitate al Ministerului Afacerilor Interne. Persoanelor juridice care nu dispun de autorizaţie pentru activitatea de pază le este

interzisă prestarea serviciilor prevăzute la art. (6).

(2) Pregătirea şi perfecţionarea cadrelor pentru activitatea de detectiv şi de pază se efectuează în centre specializate de învăţământ, stabilite de Guvern.

(3) Se interzice desfăşurarea pe teritoriul Republicii Moldova a activităţii organizaţiilor de detectiv şi de pază străine.

(4) Organizaţiilor de detectiv şi de pază străine, cetăţenilor străini şi apatrizilor li se interzice:

a) să desfăşoare activitate de detectiv şi de pază în calitate de întreprinzător individual;

b) să fondeze ori să participe ca asociat la constituirea de organizaţie de detectiv şi de pază;

c) să aibă în subordine organizaţie particulară de detectiv şi de pază ori subdiviziune specializată de pază.

Articolul 6. Genurile de activităţi particulare de detectiv şi de pază

(1) În activitatea particulară de detectiv este permisă prestarea următoarelor servicii:

a) colectarea, în bază de contract, a informaţiilor, importante pentru apărarea drepturilor şi intereselor legitime ale persoanelor fizice şi juridice;

b) colectarea de probe în cauze civile în bază de contract încheiat cu participanţii la proces;

c) studierea pieţei, colectarea de informaţii pentru negocieri, depistarea partenerilor de afaceri insolvabili sau care nu insuflă încredere;

d) protejarea întreprinderilor şi a firmelor contra spionajului industrial;

e) colectarea de date biografice sau de altă natură pentru persoana cu care se încheie contractul, cu acordul ei scris;

f) identificarea autorilor sau a expeditorilor de scrisori anonime, a colportorilor;

g) identificarea locului de aflare a persoanelor dispărute;

h) căutarea bunurilor pierdute;

i) colectarea de date în cauze penale pentru acordarea de ajutor organelor de drept în bază de contract încheiat cu participanţii la proces.

(2) În activitatea particulară de pază este permisă prestarea următoarelor servicii:

a) ocrotirea vieţii şi sănătăţii, paza bunurilor, executarea gărzii de corp;

b) paza fizică şi tehnică a localurilor şi a teritoriilor;

c) proiectarea, instalarea şi întreţinerea sistemelor de alarmare, a componentelor acestora, precum şi exploatarea dispeceratelor de monitorizare a alarmelor;

d) colectarea (încasarea) valorilor importante, precum şi transportul, paza şi însoţirea încărcăturilor/valorilor importante, a bunurilor personale;

e) patrularea, în comun cu organele de drept, a zonelor criminogene;

f) acordarea de ajutor organelor de drept la menţinerea ordinii publice, la asigurarea securităţii oamenilor;

g) informarea publicului în probleme de protecţie contra acţiunilor

ilicite.

Articolul 7. Drepturile persoanelor care practică activitate particulară de detectiv şi de pază

(1) Persoanele care practică activitate particulară de detectiv şi de pază au dreptul:

a) să presteze în bază de contract servicii de investigare şi de pază în conformitate cu legislaţia;

b) să obţină în modul stabilit informaţii şi copii de pe documente din partea persoanelor fizice şi juridice, cu acordul lor;

c) să inspecteze, după caz, cu participarea şi cu acordul proprietarului (al reprezentantului lui) teritoriul, localurile, bunurile ce îi aparţin;

d) să solicite, cu acordul clientului, concluzia specialistului în problemele care necesită cunoştinţe speciale;

e) să elucideze cauzele şi condiţiile care au condus la comiterea infracţiunilor şi să ia măsuri, în limitele competenţei, pentru lichidarea lor.

(2) Nu se admite utilizarea drepturilor acordate persoanelor fizice şi juridice care practică activitate particulară de detectiv şi de pază la îndeplinirea unor obligaţii care nu sînt prevăzute de legislaţie.

Articolul 8. Obligaţiile persoanelor care practică activitate particulară de detectiv şi de pază

(1) Persoana care practică activitate particulară de detectiv şi de pază este obligată:

a) să respecte prevederile legislaţiei şi clauzele contractuale;

b) să presteze întregul pachet de servicii prevăzute în contract;

c) să repare prejudiciile cauzate prin încălcarea clauzelor contractuale;

d) să desfăşoare activitatea cu personal atestat pentru executarea serviciilor de investigare şi de pază;

e) să păstreze confidenţialitatea informaţiei pe care o cunoaşte în procesul activităţii, să nu o utilizeze în scopuri personale şi să nu o transmită terţilor;

f) să comunice imediat organelor de drept cazurile de infracţiune depistate, să reţină la locul infracţiunii persoanele care au săvîrşit-o şi să le predea imediat organelor competente;

g) să ia măsuri urgente pentru salvarea oamenilor, pentru ajutorarea lor în protecţia bunurilor periclitate şi în alte situaţii excepţionale;

h) să prezinte organului teritorial de poliţie dare de seamă statistică. În cazul activităţii particulare de pază, aceasta va fi prezentată conform anexei nr. 1 pct. 6;

i) să plătească în termen impozitele şi taxele prevăzute de lege.

(2) Obligaţiile personalului de pază, ale conducătorilor de organizaţii, condiţiile de pază a transportului unor valori importante se stabilesc conform anexei nr. 2.

Articolul 9. Interdicţia desfăşurării activităţii particulare de detectiv şi de pază

(1) Persoanele care practică activitate particulară de detectiv şi de pază nu sînt învestite cu împuterniciri de organe de drept. Organizaţiile particulare de detectiv nu au atribuţii de urmărire penală şi nici atribuţii judecătoreşti, acestea fiind de competenţa exclusivă a organelor de urmărire penală şi a instanţelor judecătoreşti.

(2) Lucrătorii din organele de drept nu pot practica şi activitate în organizaţiile particulare de detectiv şi de pază şi în serviciile de pază interioară.

(3) Persoanele care practică activitate particulară de detectiv, de pază şi prestează servicii de pază interioară nu au dreptul să le cumuleze cu serviciul de stat.

Articolul 21. Contractul dintre detectivul particular şi client

(1) În cazul prestării de servicii, detectivul particular este obligat să încheie cu clientul contract în scris, care să cuprindă date despre părţile contractante, numărul şi data eliberării confirmării, sarcinile şi termenul lor de îndeplinire, cheltuielile aproximative şi onorariul pentru servicii, data încheierii. Contractul trebuie să conţină clauze în care părţile îşi iau angajamentul de a păstra confidenţialitatea în relaţiile lor şi îşi stabilesc răspunderea.

(2) Contractul stipulează obligaţia detectivului particular de a prezenta în scris clientului raport de activitate, la care să anexeze calculul specificat al onorariului şi al cheltuielilor pe care le-a suportat. Copia de pe raport se păstrează în arhiva detectivului în decursul a 3 ani.

Capitolul III[1]
PAZA INTERNĂ

Articolul 27[1]. Prevederi generale

Paza internă este o subdiviziune în statele de organizare a unei persoane juridice, ce dispune de un efectiv numeric de cel puţin 10 gardieni, avînd funcţie de asigurare a securităţii vieţii şi sănătăţii lucrătorilor, securităţii bunurilor aflate în proprietate.

Articolul 27[2]. Obligaţiile persoanelor încadrate în subdiviziunile de pază internă

Persoana încadrată în subdiviziunile de pază internă este obligată:

a) să respecte prevederile legislaţiei;

b) să păstreze confidenţialitatea informaţiei comerciale de care ia cunoştinţă în procesul activităţii, să nu o utilizeze în scopuri personale şi să nu o transmită terţilor;

c) să comunice imediat organelor de drept cazurile de infracţiune depistate, să reţină persoanele prinse în flagrant delict şi să le predea imediat organelor competente;

d) să ia măsuri urgente pentru salvarea oamenilor, pentru ajutorarea lor în asigurarea securităţii bunurilor periclitate şi în alte situaţii excepţionale.

PARLAMENTUL

LEGEA Nr. 264din 27-10-2005

cu privire la exercitarea profesiunii de medic

Publicat : 23-12-2005 în Monitorul Oficial Nr. 172-175 art. 839

Versiune în vigoare din 30.12.18 în baza modificărilor prin LP238 din 08.11.18 MO441-447 din 30.11.18 art. 709

Articolul 1. Obiectul de reglementare al prezentei legi

(1) Prezenta lege stabileşte bazele juridice şi reglementează condiţiile organizatorice şi formele exercitării profesiunii de medic.

(2) Prezenta lege stabileşte cerinţele faţă de persoana care doreşte să practice profesiunea de medic, drepturile, obligaţiile şi responsabilităţile generale pentru a exercita această profesiune conform jurămîntului medicului.

Articolul 3. Principiile generale ale exercitării profesiunii de medic

Principiile generale ale exercitării profesiunii de medic sînt:

a) pregătirea profesională corespunzătoare concepţiei de instruire universitară şi postuniversitară pe specialitate a cadrelor de medici şi farmacişti în Republica Moldova ajustată la standardele educaţionale profesionale internaţionale;

b) competenţa, responsabilitatea profesională a medicului şi înzestrarea lui cu înalte calităţi etico-morale, respectarea principiului „nu dăuna";

c) respectarea drepturilor şi intereselor pacientului, precum şi ale rudelor lui;

d) respectarea primatului vieţii şi a dreptului inerent la viaţă al fiinţei umane;

e) respectarea şi protejarea drepturilor şi intereselor legitime ale medicului, indiferent de caracterul public sau privat al sistemului în care activează şi de forma de exercitare a profesiunii;

f) asigurarea condiţiilor optime de exercitare a activităţii profesionale.

Articolul 13. Secretul profesional

(1) Medicul este obligat să păstreze secretul profesional.

(2) Informaţiile despre solicitarea asistenţei medicale, despre starea sănătăţii, diagnostic şi alte date obţinute de medic în examinarea şi tratamentul

pacientului constituie informaţii personale şi secretul profesional al medicului şi nu pot fi divulgate.

(3) Cu acordul pacientului sau al reprezentantului său legal, se permite transmiterea informaţiei care constituie secret profesional unor alte persoane, în interesul examinării şi tratării pacientului, al efectuării unor investigaţii ştiinţifice, utilizării acestor date în procesul de studii şi în alte scopuri.

(4) Prezentarea informaţiilor care constituie secret profesional către alte persoane fără consimţământul pacientului sau al reprezentantului său legal se admite în următoarele cazuri:

a) în scopul examinării şi tratamentului pacientului care nu este în stare, din cauza sănătăţii, să-şi exprime dorinţa;

b) în cazul posibilităţii extinderii unor maladii contagioase, intoxicaţii şi unor alte maladii care prezintă pericol în masă;

c) la cererea organelor de urmărire penală, a procuraturii şi instanţei judecătoreşti în legătură cu efectuarea urmăririi penale sau cercetării judecătoreşti;

c[1]) la cererea Avocatului Poporului sau, după caz, a Avocatului Poporului pentru drepturile copilului, în scopul asigurării protecției persoanelor împotriva torturii și a altor pedepse sau tratamente cu cruzime, inumane sau degradante.

C[2]) la solicitarea membrilor Consiliului pentru prevenirea torturii, în cadrul vizitelor efectuate de ei și în limitele necesare desfășurării vizitelor;

d) în caz de acordare a ajutorului medical unei persoane minore sau unei persoane în privinţa căreia este instituită măsura de ocrotire judiciară sub forma tutelei, incapabilă să informeze părinţii sau reprezentanţii săi legali;

în redacție prin LP238 din 08.11.18 MO441-447 din 30.11.18 art. 709

e) în cazul unor circumstanţe în al căror temei se poate presupune că prejudiciul cauzat sănătăţii persoanei reprezintă consecinţa unei acţiuni ilegale.

(5) Persoanele cărora le-au fost transmise informaţii ce constituie secret profesional poartă răspundere pentru divulgarea informaţiei transmise lor, în condiţiile legii.

(6) Secretul profesional nu poate fi divulgat nici după terminarea tratamentului sau moartea pacientului.

Articolul 17. Obligaţiile profesionale ale medicului

(1) Medicul este obligat:

e) să păstreze secretul informaţiilor personale de care a luat cunoştinţă în exercitarea profesiunii, cu excepţia cazurilor prevăzute de prezenta lege şi de legislaţia privind accesul la informaţii;

PARLAMENTUL

LEGEA Nr. 243 din 26-10-1994

Presei

Publicat : 12-01-1995 în Monitorul Oficial Nr. 2 art. 12

Articolul 1. Libertatea presei .

(1) În Republica Moldova libertatea presei constituie un drept fundamental consfinţit de Constituţie. Statul garantează tuturor persoanelor dreptul la exprimarea liberă a opiniilor şi ideilor, la informare veridică asupra evenimentelor din viaţa internă şi cea internaţională prin intermediul publicaţiilor periodice şi al agenţiilor de presă, care îşi desfăşoară activitatea în condiţiile pluralismului politic, precum şi respectarea legislaţiei cu privire la drepturile de autor.

(2) Cenzura de orice fel asupra publicaţiilor periodice şi agenţiilor de presă, imixtiunea în activitatea lor de pregătire şi de difuzare a informaţiei sînt interzise.

Articolul 2. Statutul juridic al redacţiilor publicaţiilor periodice şi al agenţiilor de presă

Redacţiile publicaţiilor. periodice şi agenţiile de presă sînt persoane juridice şi îşi desfăşoară activitatea în conformitate cu legislaţia în vigoare şi cu statutul lor.

Articolul 3. Prezentarea informaţiei de către persoanele oficiale

Persoanele oficiale ale autorităţilor publice prezintă operativ materialul şi informaţia solicitate de publicaţiile periodice şi de agenţiile de presă, exceptînd materialele şi informaţiile enumerate în art. 4 şi cele calificate drept secret de stat.

Articolul 4. Libertatea de exprimare şi limitări de publicitate

(1) Publicaţiile periodice şi agenţiile de presă publică, potrivit aprecierilor proprii, orice fel de materiale şi informaţii, ţinînd cont de faptul că exerciţiul acestor libertăţi ce comportă datorii şi responsabilităţi este supus unor formalităţi, condiţii, restrîngeri şi unor sancţiuni prevăzute de lege, care constituie măsuri necesare, intr-o societate democratică, pentru securitatea naţională, integritatea teritorială sau siguranţa publică, apărarea ordinii şi prevenirea crimei, ocrotirea sănătăţii, protecţia moralei, protecţia reputaţiei sau apărarea drepturilor altora, pentru a împiedica divulgarea unor informaţii confidenţiale sau pentru a garanta autoritatea şi imparţialitatea puterii judiciare.

(2) Publicaţiile periodice şi agenţiile de presă sînt obligate să utilizeze un limbaj accesibil şi să prezinte informaţia furnizată în aşa mod încît aceasta să nu lezeze onoarea şi demnitatea persoanelor cu dizabilităţi.

(3) Este inadmisibilă şi se contracarează în conformitate cu legislaţia în vigoare publicarea oricăror materiale şi informaţii care prezintă imaginea persoanelor cu dizabilităţi în manieră de umilinţă a demnităţii şi/sau conţine un îndemn deschis sau ascuns la discriminare, ură şi la alte acţiuni ce ar încălca drepturile acestor persoane.

Articolul 20. Drepturile şi obligaţiile jurnalistului

(1) În scopul exercitării atribuţiilor profesionale, jurnalismul are dreptul:

a) s obţină şi să difuzeze informaţii;

b) să fie primit in audienţă de persoane oficiale;

c) să facă imprimări audiovizuale, să filmeze şi să fotografieze;

d) să asiste la şedinţele publice ale instanţelor de judecată de orice nivel;

e) să aibă acces în zonele calamităţilor naturale, să asiste la mitinguri, demonstraţii şi la alte manifestaţii publice;

t) să se adreseze oricărei instituţii pentru a verifica faptele şi circumstanţele vizate în

anumite materiale;

g) să renunţe la pregătirea şi semnarea unui material, dacă acesta vine în contradicţie cu convingerile sale;

h) să-şi retragă semnătura de sub un material al cărui conţinut, după părerea sa, a fost

denaturat în procesul redactării;

i) să ceară păstrarea secretului paternităţii (de autor);

j) să beneficieze de facilităţi şi priorităţi la transport şi telecomunicaţii, la cazare în

hoteluri pe teritoriul republicii.

(2) Confiscarea notiţelor jurnalistului este interzisă. Mijloacele lui tehnice pot fi ridicate numai în cazul în care servesc drept probă într-o cauză penală .

(3) Statul garantează apărarea onoarei şi demnităţii jurnalistului, îi ocrotește sănătatea,viaţa şi bunurile.

(4) Obligaţiile jurnalistului decurg din legislaţia în vigoare, din prezenta lege şi din etica profesională.

PARLAMENTUL

LEGEA Nr. 125 din 11-05-2007

Lege privind libertatea de conştiinţă, de gîndire şi de religie

Publicat : 17-08-2007 în Monitorul Oficial Nr. 127-130 art. 546

Articolul 1. Obiectul de reglementare

Prezenta lege reglementează raporturile ce ţin de libertatea de conştiinţă de gîndire şi de religie, garantate de Constituţia Republicii Moldova şi de tratatele internaţionale în domeniul drepturilor omului la care Republica Moldova este parte, precum şi de statutul juridic al cultelor religioase şi al părţilor lor componente.

Articolul 3. Noţiuni generale

În sensul prezentei legi, se definesc următoarele noţiuni:

cult religios – structură religioasă, cu statut de persoană juridică, care îşi desfăşoară activitatea pe teritoriul Republicii Moldova conform normelor doctrinare, canonice, morale, disciplinare şi tradiţiilor istorice şi de cult proprii şi de cult proprii care nu contravin legislaţiei în vgoare, fiind constituită de către persoane supuse jurisdicţiei Republicii Moldova, care îşi manifestă în comun convingerile religioase, respectînd tradiţiile, riturile şi ceremonialul stabilit;

parte componentă a cultului religios – comunitate sau instituţie religioasă a oricărui cult religios;

comunitate religioasă – parte componentă locală a cultului religios reprezentînd o asociere de persoane care se constituie şi îşi desfăşoară activitatea pe principiile liberului consimţămînt, autonomiei, autogestiunii, egalităţii în drepturi a tuturor membrilor, creată în scopul profesării în comun a credinţei. Comunităţi religioase sînt parohiile, comunităţile monahale sau mănăstirile, congregaţiile, frăţiile,bisericile locale şi;

instituţie religioasă – parte componentă centrală sau regională a cultului religios, fondată de acesta sau de comunitatea religioasă fără consemnarea calităţii de membru, reprezentînd un aşezămînt sau o structură religioasă. Se consideră instituţii religioase eparhiile, diecezele, protopopiatele, decanatele, misiunile religioase, sociale sau de caritate, instituţiile de învăţămînt teologic de orice grad, centrele de pelerinaj, asociaţiile şi fundaţiile religioase, instanţele de disciplină bisericească, alte instituţii similare;

convingeri religioase – complex de idei, principii şi învăţături de credinţă sau dogme cu caracter religios în care o persoană crede, pe care le acceptă benevol, le mărturiseşte şi după care se conduce în viaţă;

activitate religioasă – activitate orientată spre satisfacerea necesităţilor spirituale ale credincioşilor (răspîndirea învăţăturii de credinţă, educaţia religioasă, oficierea serviciilor religioase, desfăşurarea acţiunilor de binecuvîntare şi propovăduire, instruirea şi perfecţionarea deserveţilor cultelor religioase), precum şi altă activitate orientată spre asigurarea organizatorică şi materială a practicilor de cult (editarea, desfacerea şi răspîndirea literaturii cu conţinut religios, producerea, desfacerea şi răspîndirea obiectelor de cult, confecţionarea veşmintelor de cult etc.);

credincios – persoană care crede în anumite adevăruri religioase şi care face parte benevol dintr-o comunitate religioasă cu ai cărei membri împărtăşeşte aceleaşi convingeri, aceeaşi credinţă, participă la săvîrşirea aceloraşi activităţi şi practici religioase, fiind supus unei autorităţi religioase liber alese;

conducător al cultului religios – persoană aleasă sau numită în fruntea unui cult religios, împuternicită să-l reprezinte în raporturile cu statul şi cu orice terţ;

deservent al cultului religios – persoană aleasă sau numită în funcţie în cadrul cultului religios sau al părţii lui componente;

lăcaş de cult – construcţie sau edificiu al unei comunităţi religioase în care se oficiază serviciile religioase;

obiecte de cult – obiecte folosite în cadrul serviciilor religioase, cum ar fi vasele liturgice, icoanele metalice şi cele litografice, crucile, crucifixele, mobilierul bisericesc, cruciuliţele şi medalioanele cu imagini religioase specifice cultului religios respectiv, obiectele de colportaj religios şi altele asemenea. Obiectelor de cult li se asimilează şi calendarele religioase, ilustratele, pliantele, albumele de artă bisericească, filmele, etichetele cu imaginea lăcaşurilor de cult sau a obiectelor de artă bisericească, cu excepţia celor care fac parte din patrimoniul cultural naţional, produsele necesare activităţii de cult, cum ar fi tămîia şi lumînările, inclusiv cele decorative pentru nunţi şi botezuri, stofele şi broderiile specifice folosite la confecţionarea veşmintelor de cult şi altor obiecte necesare practicării cultului respectiv;

servicii religioase – totalitate a acţiunilor religioase ce rezultă din învăţăturile de credinţă ale cultului religios respectiv;

prozelitism abuziv – acţiune de schimbare a convingerilor religioase ale unei persoane sau ale unui grup de persoane prin constrîngere.

Articolul 4. Libertatea de conştiinţă de gîndire.

(1) Orice persoană are dreptul la libertatea de gîndire, de conştiinţă şi de religie. Acest drept trebuie exercitat în spirit de toleranţă şi de respect reciproc şi cuprinde libertatea de a aparţine sau nu unei anumite religii, de a avea sau nu anumite convingeri, de a-şi schimba religia sau convingerile, de a profesa religia sau convingerile în mod individual sau în comun, în public sau în particular, prin învăţătură, practici religioase, cult şi îndeplinirea riturilor. Fiecare persoană şi comunitate religioasă poate adera liber la orice cult religios.

(2) Exercitarea dreptului la libertatea de manifestare a convingerilor sau a credinţei religioase poate fi restrînsă, în condiţiile legii, numai în cazul în care această restrîngere urmăreşte un scop legitim şi reprezintă, într-o societate democratică, măsuri necesare pentru siguranţa publică, menţinerea ordinii publice, ocrotirea sănătăţii şi a moralei publice ori pentru protejarea drepturilor şi libertăţilor persoanei.

(3) Statul exclude orice apreciere din partea sa asupra legitimităţii credinţelor religioase.

(4) Prozelitismul abuziv este interzis.

Articolul 5. Drepturi şi obligaţii generale

(1) Nimeni nu poate fi urmărit pentru convingeri, gîndire, credinţă sau necredinţă religioasă.

(2) Convingerile, gîndirea, credinţa religioasă, activitatea în cadrul unui cult religios nu pot fi un obstacol în dobîndirea şi exercitarea drepturilor civile sau politice.

Articolul 6. Libertatea de asociere religioasă

(1) Nimeni nu poate fi constrîns să practice sau nu exerciţiul religios al vreunui cult, să se asocieze sau nu la vreun cult, să contribuie sau nu la cheltuielile vreunui cult religios.

(2) Nici o comunitate religioasă nu poate fi, concomitent, parte a două sau mai multe culte religioase . Aderarea unei comunităţi religioase la un alt cult religios se poate face numai după retragerea liberă a acesteia din cultul de care a aparţinut anterior.

(3) O comunitate religioasă poate adera la orice cult religios sau se poate disocia de acesta prin voinţa liber exprimată a membrilor săi, fără aprobări suplimentare sau piedici din afară.

Articolul 11. Taina mărturisirii

Taina mărturisirii este ocrotită de lege.

Deserveţii sînt obligaţi să păstreze şi nu pot fi constrînşi să divulge faptele destăinuite în timpul oficierii tainei mărturisirii.

PARLAMENTUL

LEGEA Nr. 30 din 07-03-2013

cu privire la protecţia copiilor împotriva impactului negativ al informaţiei

Publicat : 05-04-2013 în Monitorul Oficial Nr. 69-74 art. 221

Articolul 1. Noţiuni principale

În sensul prezentei legi, următoarele noţiuni principale semnifică:

copil – persoană care nu a atins vîrsta de 18 ani (majoratul);

erotică – prezentarea, în mod artistic, a actului sexual în subiectul unui film, descrierea, în mod artistic, justificat şi fără exagerarea senzualităţii, a atracţiei sexuale sau a conduitei sexuale;

fenomen paranormal – eveniment, întîmplare, fenomen sau fapt a cărui expresie fizică nu a fost explicată de ştiinţă, aptitudini umane care nu au fost confirmate prin metode experimentale;

hipnoză – stare psihică provizorie ce constă în modificarea conştiinţei şi concentrarea bruscă asupra conţinutului unei sugestii şi/sau autosugestii, în timpul căreia se schimbă comportamentul, autocontrolul şi conştiinţa de sine a omului;

informaţie cu impact negativ asupra copiilor – informaţie accesibilă public care poate fi dăunătoare pentru sănătatea psihică şi fizică a copiilor, pentru dezvoltarea lor fizică, mintală, spirituală şi morală;

joc computerizat – program distractiv pentru calculator sau alte echipamente terminale de comunicaţii electronice, păstrat şi difuzat pe un purtător de informaţie şi/sau prin reţele computerizate publice (Internet);

pornografie – prezentarea de manieră vulgară, brutală a contactelor sexuale de orice tip între persoane de sexe diferite sau de acelaşi sex, a altor manifestări indecente ale vieţii sexuale, precum şi prezentarea de o manieră impudică a organelor genitale.

Articolul 2. Principiile de bază privind protecţia şi realizarea intereselor superioare ale copilului în sfera informaţiilor accesibile public

Principiile de bază privind protecţia şi realizarea intereselor superioare ale copilului în sfera informaţiilor accesibile public sînt:

a) interesele părinţilor (tutorilor, curatorilor), interesele obşteşti şi interesele de stat în raport cu copiii;

b) autocontrolul şi obligaţiile entităţilor care pregătesc informaţia accesibilă public, care o difuzează şi care participă la aceasta, de asemenea ale

jurnaliştilor şi organizaţiilor profesionale ale acestora;

c) coordonarea obligaţiilor şi a responsabilităţilor ce revin statului, autorităţilor publice, entităţilor care pregătesc informaţia accesibilă public, care o difuzează şi care participă la aceasta, jurnaliştilor, organizaţiilor profesionale ale acestora, precum şi părinţilor (tutorilor, curatorilor), cu privire la protecţia intereselor superioare ale copilului;

d) încurajarea difuzării informaţiei care favorizează bunăstarea socială, spirituală şi morală a copilului şi stimulează dezvoltarea lui fizică şi psihică;

e) oportunitatea, eficienţa şi proporţionalitatea măsurilor de responsabilizare;

f) raţionalitatea, onestitatea şi echitatea.

Articolul 3. Informaţia cu impact negativ asupra copiilor

(1) Se consideră informaţie cu impact negativ asupra copiilor informaţia accesibilă public:

a) despre violenţă, care încurajează agresivitatea şi dispreţul faţă de viaţă;

b) care încuviinţează deteriorarea sau nimicirea bunurilor;

c) care aduce în prim plan cadavrul sau corpul unei persoane în agonie fie un corp mutilat ca urmare a unui tratament crud, cu excepţia cazurilor în care o asemenea prezentare este necesară pentru identificarea persoanei;

d) cu caracter pornografic;

e) care invită copiii să participe la jocuri de noroc sau la alte jocuri care lasă impresia de cîştig uşor;

f) care apreciază pozitiv dependenţa faţă de substanţele stupefiante, toxice, psihotrope, tutun, alcool, precum şi faţă de alte substanţe care sînt sau pot fi utilizate drept stupefiante, şi care încurajează consumul, producerea, răspîndirea sau procurarea acestora;

g) care incită la provocarea de leziuni corporale sau la suicid, care descriu mijloacele sau circumstanţele de suicid;

h) care apreciază pozitiv o infracţiune sau care idealizează infractorii;

i) care încurajează comportamente ce jignesc demnitatea umană;

j) care relatează batjocorirea sau înjosirea unui om ori a unui grup de oameni în legătură cu originea etnică, apartenenţa naţională, rasială, sexuală, în legătură cu boala, starea socială, limba vorbită, religia practicată, convingerile sau opiniile împărtăşite;

k) care prezintă fenomene paranormale înscenate astfel încît să producă impresia realităţii;

l) care încurajează violenţa şi exploatarea sexuală, abuzurile sexuale comise asupra copiilor, relaţiile sexuale dintre copii;

m) care foloseşte limbajul licenţios şi gesturile indecente;

n) care conţine sfaturi privind producerea, procurarea sau utilizarea explozivelor, a substanţelor stupefiante ori psihotrope, a altor obiecte periculoase pentru viaţă şi sănătate;

o) care încurajează proastele deprinderi alimentare, de igienă şi

inactivitatea fizică;

p) care demonstrează o şedinţă de hipnoză în masă, al cărei subiect este auditoriul mijlocului de informare în masă.

(2) Difuzarea informaţiei cu impact negativ asupra copiilor este interzisă sau limitată în condiţiile prezentei legi.

(3) Se interzice difuzarea informaţiilor specificate la alin. (1) lit. j), precum şi a informaţiilor cu caracter pornografic care încurajează violenţa şi exploatarea sexuală a copiilor sau care au drept scop demonstrarea violenţei.

Articolul 4. Interdicţia difuzării informaţiei ce conţine date personale cu impact negativ asupra copiilor

(1) În mijloacele de informare în masă se interzice publicarea informaţiei ce conţine date cu caracter personal în cazurile în care:

a) se dau publicităţii date cu caracter personal ale unui copil bănuit, acuzat ori condamnat pentru săvîrşirea unei infracţiuni sau contravenţii, dacă acesta nu se ascunde de organele de drept ori de instanţele judecătoreşti, sau ale unui copil care este victima unei infracţiuni ori contravenţii, ceea ce permite identificarea acestuia;

b) se dau publicităţii datele cu caracter personal ale unui copil care fie şi-a provocat leziuni corporale ori a încercat să o facă, fie s-a sinucis ori a făcut o tentativă de sinucidere, ceea ce permite identificarea acestuia;

c) se prezintă fotografii ale copiilor sau materiale video despre aceştia în contextul unor fenomene sociale negative, ceea ce permite identificarea copiilor;

d) informaţia respectivă jigneşte demnitatea copilului identificat şi/sau lezează interesele sale superioare.

(2) În serviciile de programe radio şi televizate se interzice difuzarea informaţiei cu impact negativ asupra copiilor ce conţine:

a) imagini ori fotografii ale corpului copilului decedat;

b) imagini de natură pornografică;

c) orice referire defavorabilă sau discriminatorie la originea etnică, naţionalitatea, rasa ori religia unui copil, precum şi la dizabilitatea acestuia;

d) orice indicii care ar putea duce la identificarea copiilor implicaţi în situaţii cu conotaţie negativă (accidente, infracţiuni, abuz sexual, abuz fizic sau psihic, dispute familiale, sinucideri, consum de droguri, abuz de alcool etc.), inclusiv în calitate de victime sau martori. Fac excepţie situaţiile în care jurnalistul acţionează cu acordul părinţilor (tutorilor, curatorilor) în interesul superior al copilului;

e) orice indicii care ar putea duce la identificarea unui copil implicat în acte de autovătămare corporală de orice natură, inclusiv în tentative de suicid sau în sinucideri;

f) orice indicii care ar putea duce la identificarea unui copil infectat cu HIV sau bolnav de SIDA. Această interdicţie se aplică chiar şi atunci cînd intenţia programului este de a prezenta şi de a pune în evidenţă o problemă socială;

g) reconstituiri ale infracţiunilor, abuzurilor şi ale altor situaţii cu conotaţie negativă în care sînt folosiţi copiii;

h) interviuri şi declaraţii în care copiilor le sînt solicitate păreri referitoare la probleme intime de familie sau probleme care le depăşesc puterea de judecată.

(3) În cazul copiilor cu vîrsta cuprinsă între 16 şi 18 ani, aflaţi în diferite forme de detenţie (reţinut, arestat, deţinut în penitenciar) sau care au calitatea procesuală de bănuit, învinuit, inculpat sau condamnat pentru comiterea unor infracţiuni în cadrul unei urmăriri penale, fie în cazul copiilor victime sau martori ale abuzurilor fizice, psihice sau sexuale, aceştia pot apărea în programele audiovizuale dacă sînt îndeplinite cumulativ următoarele condiţii:

a) există acordul scris al copilului;

b) au fost luate măsuri de protecţie a identităţii copilului.

Articolul 5. Limitarea răspîndirii informaţiei cu impact negativ asupra copiilor

(1) Pentru a permite părinţilor (tutorilor, curatorilor) copiilor să facă alegerea potrivită, toţi radiodifuzorii au obligaţia să pună la dispoziţia publicului informaţii suficiente privind intervalul orar de difuzare, recomandările şi avertizările sonore şi vizuale, astfel încît programele vizionate sau ascultate în familie sau numai de către copii să nu afecteze dezvoltarea fizică, mintală, spirituală sau morală a acestora. Aceleaşi obligaţii sînt valabile în cazul serviciilor de programe retransmise de către radiodifuzori.

(2) Radiodifuzorilor le este interzisă difuzarea în intervalul orar 6.00 – 20.00 de programe audiovizuale de studio sau realizate în direct în care se fumează, se consumă băuturi alcoolice ori se prezintă acte de comportament obscen.

(3) Mijloacele de informare în masă nu pot difuza în intervalul orar 6.00 – 23.00 producţii care prezintă:

a) violenţă fizică, psihică sau de limbaj în mod repetat;

b) scene de sex, de limbaj sau de comportament obscen;

c) persoane în ipostaze degradante;

d) lupte libere nereglementate de federaţiile sportive naţionale sau internaţionale.

(4) Programele de ştiri şi de actualităţi se supun cerinţelor de protecţie a copiilor şi vizionării în familie. În cazul difuzării unor scene de violenţă sau cu impact emoţional negativ, avertizarea verbală a publicului este obligatorie. Mijloacele de informare în masă nu pot prezenta scene de violenţă în mod repetat în cadrul aceleiaşi producţii audiovizuale, iar imaginile care prezintă execuţii, oameni ucişi sau voluntari ai morţii, indiferent de motivaţia acestora, se difuzează numai în cazuri temeinic justificate.

(5) Programele audiovizuale care pot afecta dezvoltarea fizică, mintală, spirituală sau morală a copiilor pot fi difuzate numai dacă vizionarea este

restricţionată printr-un sistem de acces condiţionat. În lipsa unui sistem de acces condiţionat, difuzarea programelor respective se poate face numai în intervalul orar permis, potrivit clasificării programului în funcţie de conţinutul acestuia. Responsabilitatea clasificării acestor producţii audiovizuale le revine titularilor de licenţă de emisie.

(6) Categoriile în care se încadrează producţiile audiovizuale ce pot afecta dezvoltarea fizică, mintală sau morală a copiilor sînt următoarele:

a) producţii audiovizuale interzise copiilor sub 18 ani – se difuzează numai în intervalul orar 24.00 – 6.00 şi vor fi însoţite permanent de un semn de avertizare reprezentînd un cerc de culoare roşie, iar în interiorul acestuia, pe fond transparent, numărul **18** de culoare albă;

b) producţii audiovizuale interzise copiilor sub 15 ani – se difuzează numai în intervalul orar 22.00 – 6.00 şi vor fi însoţite permanent de un semn de avertizare reprezentînd un cerc de culoare roşie, iar în interiorul acestuia, pe fond transparent, numărul **15** de culoare albă;

c) producţii audiovizuale interzise copiilor sub 12 ani – se difuzează numai după ora 20.00 şi vor fi însoţite de un semn de avertizare reprezentînd un cerc de culoare roşie, iar în interiorul acestuia, pe fond transparent, numărul **12** de culoare albă;

d) producţii audiovizuale interzise copiilor sub 7 ani – se difuzează numai după ora 20.00 şi vor fi însoţite de un semn de avertizare reprezentînd un cerc de culoare roşie, iar în interiorul acestuia, pe fond transparent, numărul **7** de culoare albă;

e) producţii audiovizuale care pot fi vizionate de copiii în vîrstă de pînă la 12 ani numai cu acordul sau împreună cu părinţii ori familia – se difuzează însoţite de un semn de avertizare reprezentînd un cerc de culoare roşie, iar în interiorul acestuia, pe fond transparent, majusculele **AP**(acord parental) de culoare albă.

(7) În clasificarea producţiilor cinematografice, radiodifuzorii se vor ghida şi de clasificarea stabilită de producător sau, după caz, de clasificarea sub care producţia a fost difuzată în alte ţări.

(8) Furnizorii de servicii de acces la Internet vor oferi utilizatorilor finali posibilitatea de instalare a aplicațiilor de filtrare a conținutului din Internet cu impact negativ asupra copiilor, de asemenea vor introduce în meniul principal al paginilor web oficiale ale lor un compartiment dedicat informațiilor privind siguranţa pe Internet.

in redacție prin LP164 din 26.07.18, MO333-335/24.08.18 art.543

(9) Producătorii şi/sau difuzorii de jocuri computerizate vor marca jocurile computerizate cu un indice de vîrstă în modul stabilit de Guvern.

(10) Restricţiile privind difuzarea informaţiei cu impact negativ asupra copiilor se aplică de asemenea publicităţii, autopublicităţii, mărcilor comerciale, jocurilor computerizate şi altor informaţii accesibile public.

Articolul 6. Excepţii de la restricţiile privind difuzarea informaţiei cu impact negativ asupra copiilor

(1) Informaţia cu impact negativ asupra copiilor poate fi difuzată fără respectarea restricţiilor stabilite la art. 5 dacă:

a) această informaţie are valoare ştiinţifică sau artistică fie este necesară pentru cercetări, instruire sau educaţie;

b) publicarea ei se face în interes public.

(2) Programele, emisiunile sau părţi ale acestora care fac uz de excepţiile prevăzute la alin. (1) vor fi precedate de un aviz privind posibilul lor impact negativ asupra copiilor.

Articolul 7. Autorităţile abilitate cu realizarea dispoziţiilor prezentei legi

(1) Supravegherea realizării dispoziţiilor prezentei legi se efectuează de către:

a) Consiliul Coordonator al Audiovizualului;

c) Ministerul Educației, Culturii și Cercetării;

d) Ministerul Sănătății, Muncii și Protecției Sociale;

e) Ministerul Economiei și Infrastructurii;

f) Ministerul Afacerilor Interne;

g) autoritățile administrației publice locale.

(2) Consiliul Coordonator al Audiovizualului şi atribuie informaţiilor accesibile public calitatea de informaţie cu impact negativ asupra copiilor.

(3) Deciziile Consiliului Coordonator al Audiovizualului se adoptă, se publică și se atacă în modul prevăzut de legislația în vigoare.

(5) Autorităţile specificate la alin. (1) colaborează între ele, fac schimb de informaţii şi sesizează organele de specialitate cu privire la nerespectarea dispoziţiilor prezentei legi.

(6) Persoanele interesate pot sesiza orice autoritate responsabilă privind încălcarea prezentei legi.

Articolul 8. Răspunderea pentru încălcarea dispoziţiilor prezentei legi

Încălcarea dispoziţiilor prezentei legi se sancţionează conform prevederilor legislaţiei în vigoare.

PARLAMENTUL

LEGEA Nr. 20 din 03-02-2009

privind prevenirea şi combaterea criminalităţii informatice

Publicat : 26-01-2010 în Monitorul Oficial Nr. 11-12 art. 17

Versiune în vigoare din 15.06.18 în baza modificărilor prin LP79 din 24.05.18, MO195-209/15.06.18 art.338

Articolul 1. Obiectul de reglementare

Prezenta lege reglementează raporturile juridice privind:

a) prevenirea şi combaterea infracţiunilor informatice;

b) cadrul de asistenţă mutuală în prevenirea şi combaterea criminalităţii informatice, în protecţia şi acordarea de ajutor furnizorilor de servicii şi utilizatorilor de sisteme informatice;

c) colaborarea autorităţilor administraţiei publice cu organizaţii negu-vernamentale şi cu alţi reprezentanţi ai societăţii civile în activitatea de prevenire şi de combatere a criminalităţii informatice;

d) cooperarea cu alte state, cu organizaţii internaţionale şi regionale avînd competenţe în domeniu.

Articolul 2. Noţiuni principale

În sensul prezentei legi, următoarele noţiuni principale semnifică:

sistem informatic – orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor;

date informatice – orice reprezentare de fapte, informaţii sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcţii de către un sistem informatic;

furnizor de servicii – orice entitate publică sau privată care oferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic, precum şi orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicaţii sau pentru utilizatorii săi;

date referitoare la trafic – orice date avînd legătură cu o comunicare transmisă printr-un sistem informatic, produse de acest sistem în calitate de element al lanţului de comunicare, indicînd originea, destinaţia, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent;

date referitoare la utilizatori- orice informaţie, sub formă de date informatice sau sub orice altă formă, deţinută de un furnizor de servicii, referitoare la abonaţii acestor servicii, altele decît datele referitoare la trafic sau conţinut, şi care permit stabilirea: tipului de serviciu de comunicaţii utilizat, dispoziţiilor tehnice luate în această privinţă şi peroadei serviciului; identităţii, adresei poştale sau geografice, numărului de telefon al abonatului şi oricărui alt număr de contact, precum şi a datelor referitoare la facturare şi plată, disponibile în baza unui contract sau a unui aranjament de servicii; oricărei alte informaţii referitoare la locul în care se găsesc echipamentele de comunicate, disponibile în baza unui contract sau a unui aranjgment de servicii, precum şi a oricăror alte date care pot conduce la identificarea utilizatorului**;**

măsuri de securitate – folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori.

Articolul 3. Principiile de bază ale prevenirii şi combaterii criminalităţii informatice

Prevenirea şi combaterea criminalităţii informatice se efectuează pe următoarele principii:

a) legalitatea;

b) respectarea drepturilor şi libertăţilor fundamentale ale omului;

c) operativitatea;

d) inevitabilitatea pedepsei;

e) securitatea informatică şi protecţia datelor cu caracter personal;

f) utilizarea complexă a măsurilor de profilaxie: juridice, social-economice şi informatice;

g) parteneriatul social, colaborarea autorităţilor administraţiei publice cu organizaţii internaţionale, cu organizaţii neguvernamentale, cu alţi reprezentanţi ai societăţii civile.

Capitolul II

CADRUL INSTITUŢIONAL

Articolul 4. Funcţiile autorităţilor şi instituţiilor publice competente în domeniul prevenirii şi combaterii criminalităţii informatice

(1) Ministerul Afacerilor Interne, şi Serviciul de Informaţii şi

Securitate formează şi actualizează în permanenţă bazele de date privind criminalitatea informatică.

(2) Ministerul Afacerilor Interne efectuează măsuri speciale de investigaţie, de urmărire penală, de cooperare internaţională, de identificare a persoanelor care comit infracţiuni informatice.

(3) Serviciul de Informaţii şi Securitate desfăşoară activităţi de prevenire şi combatere a criminalităţii informatice ce prezintă ameninţări la adresa securităţii naţionale, activităţi operative de investigaţii, de depistare a legăturilor organizaţiilor criminale internaţionale, alte activităţi în limita competenţei sale.

(4) Procuratura Generală:

a) coordonează, conduce şi exercită urmărirea penală, în modul prevăzut de lege;

b) dispune, în cadrul desfăşurării urmăririi penale, la solicitarea organului de urmărire penală sau din oficiu, conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, faţă de care există pericolul distrugerii ori alterării, în condiţiile legislaţiei de procedură penală;

c) reprezintă învinuirea, în numele statului, în instanţă de judecată în modul prevăzut de lege.

(5) Ministerul Economiei şi Infrastructurii , în comun cu Serviciul de Informaţii şi Securitate, prezintă propuneri privind asigurarea protecţiei şi securităţii informatice.

(6) Institutul Naţional al Justiţiei realizează perfecţionarea profesională a personalului antrenat în înfăptuirea justiţiei în domeniul combaterii criminalităţii informatice.

substituit prin LP79 din 24.05.18, MO195-209/15.06.18 art.338

Articolul 5. Colaborarea autorităţilor competente în prevenirea şi combaterea criminalităţii informatice

În cadrul activităţilor de prevenire şi combatere a criminalităţii informatice, autorităţile competente, furnizorii de servicii, organizaţiile neguvernamentale, alţi reprezentanţi ai societăţii civile colaborează prin schimb de informaţii, de experţi, prin activităţi comune de cercetare a cazurilor şi de identificare a infractorilor, de instruire a personalului, prin realizarea de iniţiative în scopul promovării unor programe, practici, măsuri, proceduri şi standarde minime de securitate a sistemelor informatice, prin campanii de informare privind criminalitatea informatică şi riscurile la care sînt expuşi utilizatorii de sisteme informatice, prin alte activităţi în domeniu.

Articolul 6. Obligaţiile proprietarilor de sisteme informatice

Proprietarii de sisteme informatice accesul la care este interzis sau restricţionat pentru anumite categorii de utilizatori au obligaţia de a avertiza utilizatorii referitor la condiţiile legale de acces şi de utilizare, precum şi la consecinţele juridice ale accesului nesancţionat la aceste sisteme informatice. Avertizarea trebuie să fie accesibilă oricărui utilizator.

Articolul 7. Obligaţiile furnizorilor de servicii

(1) Furnizorii de servicii sînt obligaţi:

a) să ţină evidenţa utilizatorilor de servicii;

b) să comunice autorităţilor competente datele despre traficul informatic, inclusiv datele despre accesul ilegal la informaţia din sistemul informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau cu gradul ei de protecţie, dacă acestea au contribuit la însuşirea, la denaturarea sau la distrugerea informaţiei ori au provocat alte urmări grave, perturbarea funcţionării sistemelor informatice, alte delicte informatice;

c) să execute, în condiţii de confidenţialitate, solicitarea autorităţii competente privind conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, faţă de care există pericolul distrugerii ori alterării, pe un termen de pînă la 120 de zile calendaristice, în condiţiile legislaţiei naţionale;

d) să prezinte autorităţilor competente, în temeiul unei solicitări efectuate în condiţiile legii, date referitoare la utilizatori, inclusiv la tipul de comunicaţie şi la serviciul de care a beneficiat utilizatorul, la modalitatea de plată a serviciului**;**

e) să întreprindă măsuri de securitate prin utilizarea unor proceduri, dispozitive sau programe informatice specializate cu al căror ajutor accesul la un sistem informatic să fie restricţionat sau interzis utilizatorilor neautorizaţi;

f) să asigure monitorizarea, supravegherea şi păstrarea datelor referitoare la trafic, pe o perioadă de 180 de zile calendaristice, pentru identificarea furnizorilor de servicii, utilizatorilor de servicii şi a canalului prin al cărui intermediu comunicaţia a fost transmisă;

g) să asigure descifrarea datelor informatice care se conţin în pachetele protocoalelor de reţea cu conservarea acestor date pe o perioadă de 90 de zile calendaristice.

(2) În cazul în care datele referitoare la traficul informatic se află în posesia mai multor furnizori de servicii, furnizorul de servicii solicitat este obligat să pună de îndată la dispoziţia autorităţii competente informaţia necesară identificării celorlalţi furnizori de servicii.

Capitolul III

COOPERAREA INTERNAŢIONALĂ

Articolul 8. Cooperarea internaţională a autorităţilor competente

(1) Autorităţile competente colaborează, în condiţiile legii, respectînd obligaţiile prevăzute de tratatele internaţionale la care Republica Moldova este parte, cu instituţiile care au atribuţii similare din alte state, precum şi cu organizaţiile internaţionale specializate în domeniu.

(2) Colaborarea prevede: asistenţa juridică internaţională în materie penală; extrădarea; identificarea; blocarea, sechestrarea şi confiscarea produselor şi a instrumentelor infracţiunii; desfăşurarea anchetelor comune; schimbul de informaţii; formarea personalului de specialitate; alte activităţi similare.

Articolul 9. Activitatea operativă de investigaţii şi de urmărire penală desfăşurată în comun

(1) La solicitarea autorităţilor naţionale competente sau ale altor state, pe teritoriul Republicii Moldova se pot desfăşura, în condiţiile legii, activităţi operative de investigaţii în cadrul urmăririi penale comune în vederea prevenirii şi combaterii criminalităţii informatice.

(2) Anchetele comune se vor desfăşura şi în bază de acorduri bilaterale sau multilaterale încheiate de autorităţile competente.

(3) Reprezentanţii autorităţilor competente din Republica Moldova pot participa la anchete comune desfăşurate pe teritoriul unor alte state, cu respectarea legislaţiei lor.

Articolul 10. Solicitările autorităţilor competente străine

(1) În cadrul cooperării internaţionale, autoritatea competentă străină poate solicita autorităţii competente din Republica Moldova conservarea imediată a datelor informatice sau a datelor privind traficul informatic, existente într-un sistem informatic de pe teritoriul Republicii Moldova, referitor la care autoritatea competentă străină urmează să formuleze o cerere, argumentată, de asistenţă juridică internaţională în materie penală.

(2) Cererea de conservare imediată prevăzută la alin.(l) cuprinde:

a) denumirea autorităţii care solicită conservarea;

b) prezentarea succintă a faptelor care fac obiectul urmăririi penale şi argumentarea lor juridică;

c) datele informatice care se solicită a fi conservate;

d) orice informaţie disponibilă, necesară identificării deţinătorului de date informatice, localizarea sistemului informatic;

e) utilitatea datelor informatice, necesitatea conservării lor;

f) intenţia autorităţii competente străine de a formula o cerere de asistenţă juridică internaţională în materie penală.

(3) Termenul de conservare a datelor consemnate la alin.(l) nu poate fimai mic de 60 de zile calendaristice şi este valabil pînă cînd autorităţile competente naţionale decid asupra cererii de asistenţă juridică internaţională în materie penală.

(4) Transmiterea datelor informatice se va efectua doar în urma acceptării cererii de asistenţă juridică internaţională în materie penală.

Capitolul IV

RĂSPUNDEREA

Articolul 11. Răspunderea pentru încălcarea prezentei legi

Încălcarea prezentei legi atrage răspundere disciplinară, civilă, contravenţională sau penală, în condiţiile legii.

PARLAMENTUL

LEGEA Nr. 91din 27-06-2014

privind semnătura electronică şi documentul electronic

Publicat : 04-07-2014 în Monitorul Oficial Nr. 174-177 art. 397

MODIFICAT LP317 din 30.11.18, MO1-5/04.01.19 art.40; în vigoare 04.02.19

Articolul 1. Scopul legii şi domeniul de aplicare

(1) Prezenta lege stabileşte regimul juridic al semnăturii electronice şi al documentului electronic, inclusiv cerinţele principale faţă de valabilitatea acestora şi cerinţele principale faţă de serviciile de certificare.

(2) Prezenta lege nu limitează modul de utilizare a documentelor.

(3) Recunoaşterea semnăturii electronice şi a documentului electronic în afara Republicii Moldova este reglementată de tratatele internaţionale la care Republica Moldova este parte. În cazul în care tratatele internaţionale la care Republica Moldova este parte stabilesc alte norme decît cele prevăzute de prezenta lege, se aplică normele tratatelor internaţionale.

Articolul 2. Noţiuni principale

În sensul prezentei legi, următoarele noţiuni semnifică:

acreditare voluntară – autorizaţie care prevede drepturi şi obligaţii specifice prestării de servicii de certificare, acordată, la cererea prestatorului de servicii de certificare, de către organul competent responsabil de stabilirea drepturilor şi obligaţiilor respective şi de supravegherea respectării acestora, în cazul în care prestatorul de servicii de certificare nu este împuternicit să exercite drepturile care decurg din autorizaţie pînă nu a primit decizia organului respectiv;

arhiva electronică securizată – depozit structurat de documente electronice, care asigură confidenţialitatea, nonrepudierea şi integritatea acestora şi care garantează valoarea probantă în timp a documentelor electronice;

autenticitate a documentului electronic – calitate a documentului electronic care constă în faptul că acesta este semnat de persoana care deţine o semnătură electronică autentică şi este abilitată cu drept de semnătură;

certificat al cheii publice – document electronic ce conţine cheia publică, este semnat cu semnătura electronică a prestatorului de servicii de certificare, atestă apartenenţa cheii respective titularului de certificat al cheii publice şi permite identificarea acestui titular;

certificat calificat al cheii publice – certificat al cheii publice care întruneşte cerinţele prevăzute la art.31 şi este eliberat de un prestator de servicii de certificare ce întruneşte cerinţele prevăzute la art.26;

cheie privată – consecutivitate digitală unică, formată prin intermediul dispozitivului de creare a semnăturii electronice şi destinată a fi utilizată pentru crearea semnăturii electronice;

cheie publică – consecutivitate digitală unică, formată prin intermediul dispozitivului de creare a semnăturii electronice, care corespunde cheii private interdependente şi este destinată a fi utilizată pentru verificarea autenticităţii semnăturii electronice;

circulaţie electronică a documentelor – totalitatea proceselor de creare, prelucrare, expediere, recepţionare, păstrare, modificare şi/sau nimicire a documentelor electronice;

date de creare a semnăturii electronice – date unice, precum codurile sau cheile private, care sînt utilizate de semnatar pentru crearea unei semnături electronice;

date de verificare a semnăturii electronice – date, precum codurile sau cheile publice, care sînt utilizate în scopul verificării unei semnături electronice;

dispozitiv de creare a semnăturii electronice – mijloace tehnice şi/sau de program configurate, utilizate pentru punerea în aplicare a datelor de creare a semnăturii electronice;

dispozitiv securizat de creare a semnăturii electronice – dispozitiv de creare a semnăturii electronice care întruneşte cerinţele prevăzute la art.8 alin. (3) şi (4);

dispozitiv de verificare a semnăturii electronice – mijloace tehnice şi/sau de program configurate, utilizate pentru punerea în aplicare a datelor de verificare a semnăturii electronice;

destinatar al documentului electronic – persoană fizică sau juridică căreia îi este adresat documentul electronic sau altă persoană care, în condiţiile legii sau ale contractului, recepţionează documentul electronic;

document electronic – informaţie în formă electronică, creată, structurată, prelucrată, păstrată şi/sau transmisă prin intermediul computerului sau al altor dispozitive electronice, semnată cu semnătură electronică în conformitate cu prezenta lege;

intermediar în circulaţia electronică a documentelor – întreprinzător individual sau persoană juridică care, din însărcinarea semnatarului şi/sau a destinatarului documentului electronic, organizează şi administrează sistemul de circulaţie electronică a documentelor şi/sau prestează servicii legate de circulaţia electronică a documentelor;

marcă temporală – atribut al documentului electronic, care, prin intermediul semnăturii electronice, certifică faptul că informaţia a existat la un moment de timp determinat, cu păstrarea autenticităţii şi integrităţii documentului electronic;

prestator de servicii de certificare – întreprinzător individual sau persoană juridică care prestează servicii de certificare;

produs asociat semnăturii electronice – mijloace tehnice sau de program ori componente specifice ale acestora, destinate a fi utilizate de către un prestator de servicii de certificare la prestarea serviciilor de certificare sau destinate a fi utilizate pentru crearea ori verificarea semnăturilor electronice;

Registrul împuternicirilor de reprezentare în baza semnăturii electronice – registru ţinut în formă electronică în care sînt consemnate împuternicirile de reprezentare în baza semnăturii electronice acordate de către persoane fizice sau juridice unei alte persoane;

semnatar – persoană care deţine un dispozitiv de creare a semnăturii electronice şi care acţionează fie în nume propriu, fie în numele persoanei fizice, al persoanei juridice sau al entităţii pe care o reprezintă;

semnătură electronică – date în formă electronică, care sînt ataşate la sau logic asociate cu alte date în formă electronică şi care sînt utilizate ca metodă de autentificare;

servicii de certificare – servicii de certificare a cheilor publice, de aplicare a mărcii temporale, alte servicii conexe în domeniul semnăturii electronice;

sistemul de circulaţie electronică a documentelor – sistem tehnico-organizatoric ce asigură circulaţia documentelor electronice.

Capitolul II
REGIMUL JURIDIC AL SEMNĂTURII ELECTRONICE

Articolul 3. Principiile de utilizare a semnăturii electronice

Principiile de utilizare a semnăturii electronice sînt următoarele:

a) libertatea alegerii şi utilizării oricărui tip de semnătură electronică, dacă actele normative sau acordul părţilor nu prevăd cerinţa de utilizare a unui tip concret de semnătură electronică, în corespundere cu obiectivele de utilizare a acesteia;

b) posibilitatea alegerii oricăror tehnologii şi/sau mijloace tehnice care permit utilizarea tipurilor concrete de semnături electronice în conformitate cu prevederile prezentei legi;

c) neadmiterea invocării lipsei de putere juridică a semnăturii electronice şi/sau a documentului electronic semnat prin intermediul acesteia doar în baza faptului că semnătura electronică nu a fost creată manual, dar prin intermediul dispozitivului de creare a semnăturii şi/sau al produsului asociat semnăturii electronice.

Articolul 4. Tipuri de semnături electronice

(1) Tipurile de semnături electronice, ale căror principii şi mecanisme de utilizare sînt reglementate de prezenta lege, sînt următoarele:

a) semnătura electronică simplă;

b) semnătura electronică avansată necalificată;

c) semnătura electronică avansată calificată.

(2) Semnătura electronică simplă este semnătura electronică utilizată ca metodă de autentificare, fără a face trimitere exclusiv la semnatar.

(3) Semnătura electronică avansată necalificată este o semnătură electronică ce îndeplineşte următoarele cerinţe:

a) face trimitere exclusiv la semnatar;

b) permite identificarea semnatarului;

c) este creată prin mijloace controlate exclusiv de semnatar; şi

d) este legată de datele la care se raportează, astfel încît orice modificare ulterioară a acestor date poate fi detectată.

(4) Semnătura electronică avansată calificată este o semnătură electronică care îndeplineşte toate cerinţele semnăturii electronice avansate necalificate şi, suplimentar:

a) se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate;

b) este creată prin intermediul dispozitivului securizat de creare a semnăturii electronice şi se verifică securizat cu ajutorul dispozitivului de verificare a semnăturii electronice şi/sau al produsului asociat semnăturii electronice, care dispun de confirmarea corespunderii cu cerinţele prevăzute de prezenta lege.

Articolul 5. Regimul juridic de utilizare a semnăturii electronice

(1) Semnătura electronică, indiferent de gradul de protecţie de care dispune, produce efecte juridice şi este acceptată ca probă, inclusiv în cadrul procedurilor judiciare, chiar dacă:

a) se prezintă în formă electronică; sau

b) nu se bazează pe un certificat eliberat de un prestator acreditat de servicii de certificare; sau

c) nu se bazează pe un certificat calificat al cheii publice; sau

d) nu este creată prin intermediul dispozitivului securizat de creare a semnăturii electronice.

(2) Semnătura electronică avansată calificată are aceeaşi valoare juridică ca şi semnătura olografă.

(3) Modalitatea în care se va asigura gradul de protecţie a semnăturii electronice avansate calificate pentru echivalarea acesteia cu semnătura olografă aplicată pe hîrtie se stabileşte de organul competent, conform atribuţiilor prevăzute la art.36 alin.(1).

(4) Modalitatea de aplicare a semnăturilor electronice de către funcţionarii persoanelor juridice de drept public se stabileşte de Guvern. Persoanele juridice de drept privat stabilesc de sine stătător modalitatea de aplicare a semnăturilor electronice de către reprezentanţii acestora.

(5) Semnătura electronică nu constituie un mijloc de criptare a informaţiei.

Articolul 6. Recunoaşterea semnăturilor electronice străine

(1) Certificatul cheii publice eliberat de către un prestator de servicii de

certificare cu domiciliul sau cu sediul într-un alt stat este recunoscut ca fiind echivalent, din punctul de vedere al efectelor juridice, cu certificatul cheii publice eliberat de un prestator de servicii de certificare cu domiciliul sau cu sediul în Republica Moldova dacă este întrunită una dintre următoarele condiţii:

a) prestatorul de servicii de certificare cu domiciliul sau cu sediul în alt stat a fost acreditat în cadrul regimului de acreditare în conformitate cu prevederile prezentei legi;

b) un prestator de servicii de certificare acreditat cu domiciliul sau cu sediul în Republica Moldova garantează recunoaşterea certificatului;

c) certificatul sau prestatorul de servicii de certificare care l-a eliberat este recunoscut prin aplicarea unui acord bilateral sau multilateral între Republica Moldova şi alte state sau organizaţii internaţionale, pe bază de reciprocitate.

(2) Semnătura electronică şi documentul electronic semnat cu semnătură electronică nu pot fi considerate lipsite de putere juridică doar în baza faptului că certificatul cheii publice a fost eliberat în corespundere cu normele unui stat străin.

Articolul 7. Cheia privată şi cheia publică

(1) Cheia privată şi cheia publică utilizate la crearea semnăturii electronice avansate necalificate se creează de către persoana fizică. Acestea pot fi create de persoane terţe, prin acordul expres al persoanei fizice respective, cu condiţia asigurării imposibilităţii de copiere a acestor chei.

(2) Cheia privată şi cheia publică utilizate la crearea semnăturii electronice avansate calificate se creează de către prestatorul de servicii de certificare prin intermediul dispozitivului securizat de creare a semnăturii. În cazul utilizării dispozitivului securizat de creare a semnăturii în baza cartelei SIM, prestatorul de servicii de certificare asigură persoanei fizice iniţierea procedurii de creare a cheii private şi a cheii publice.

(3) Cheia privată şi cheia publică interdependente se creează concomitent.

(4) Persoana fizică poate fi titular al unui număr nelimitat de chei private şi chei publice.

(5) Cheia privată este păstrată şi utilizată exclusiv de către titular, într-un mod ce exclude accesul la ea al altei persoane.

(6) Cheia publică este certificată de către prestatorul de servicii de certificare şi este accesibilă tuturor.

Articolul 8. Crearea semnăturii electronice

(1) Crearea semnăturii electronice se efectuează prin intermediul dispozitivului de creare a semnăturii electronice şi/sau al produsului asociat semnăturii electronice, cu utilizarea datelor de creare a semnăturii electronice.

(2) La crearea semnăturii electronice simple, părţile se bazează pe prevederile acordului încheiat.

(3) La crearea semnăturii electronice avansate necalificate şi a semnăturii electronice avansate calificate, dispozitivul de creare a semnăturii electro-

nice şi/sau produsul asociat semnăturii electronice trebuie:

a) să ofere posibilitatea afişării conţinutului documentului electronic semnat cu semnătura electronică sau să facă referinţa irevocabilă la documentul dat;

b) să creeze o semnătură electronică numai după confirmarea de către semnatar a operaţiunii de creare a semnăturii electronice;

c) să confirme în mod univoc crearea semnăturii electronice.

(4) Dispozitivele securizate de creare a semnăturii electronice trebuie să asigure, prin mijloace tehnice şi proceduri corespunzătoare, cel puţin că:

a) datele de creare a semnăturii electronice nu pot apărea decît o singură dată, iar confidenţialitatea acestora este asigurată în conformitate cu prezenta lege;

b) datele de creare a semnăturii electronice nu pot fi deduse prin calcul şi semnătura este protejată împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată;

c) datele de creare a semnăturii electronice sînt protejate în mod fiabil de semnatarul legitim împotriva utilizării de către alte persoane.

(5) Dispozitivele securizate de creare a semnăturii electronice nu trebuie să modifice datele care urmează a fi semnate sau să împiedice prezentarea lor semnatarului înainte de semnare.

Articolul 9. Verificarea autenticităţii semnăturii electronice

(1) Verificarea autenticităţii semnăturii electronice se efectuează prin intermediul dispozitivului de verificare a semnăturii electronice şi/sau al produsului asociat semnăturii electronice, cu utilizarea datelor de verificare a semnăturii electronice.

(2) La verificarea semnăturii electronice simple, părţile se bazează pe prevederile acordului încheiat, care trebuie să prevadă modalitatea de confirmare a integrităţii documentului electronic semnat.

(3) La verificarea semnăturii electronice avansate necalificate şi semnăturii electronice avansate calificate, dispozitivul de verificare a semnăturii electronice şi/sau produsul asociat semnăturii electronice trebuie:

a) să ofere posibilitatea afişării conţinutului documentului electronic semnat cu semnătura electronică sau să facă referinţa irevocabilă la documentul dat;

b) să afişeze faptul modificării documentului electronic semnat cu semnătura electronică;

c) să facă referinţă la semnatar.

(4) La verificarea securizată a semnăturii electronice avansate necalificate şi a semnăturii electronice avansate calificate trebuie să se garanteze, cu o siguranţă suficientă, că:

a) datele de verificare a semnăturii electronice corespund datelor afişate persoanei care verifică semnătura electronică;

b) semnătura electronică este verificată cu certitudine, iar rezultatul verificării şi identitatea semnatarului sînt corect afişate;

c) autenticitatea şi valabilitatea certificatului cheii publice solicitat în momentul verificării semnăturii electronice sînt verificate cu certitudine;

d) conţinutul certificatului cheii publice este redat clar; şi

e) orice modificări care pot influenţa securitatea semnăturii electronice pot fi detectate.

Articolul 10. Utilizarea semnăturii electronice simple

(1) Documentul electronic se consideră semnat cu semnătura electronică simplă dacă este întrunită una dintre următoarele condiţii:

a) semnătura electronică simplă se conţine nemijlocit în documentul electronic sau este logic asociată cu documentul electronic;

b) datele de creare a semnăturii electronice simple se aplică în corespundere cu regulile stabilite de către operatorul sistemului informatic prin intermediul căruia se efectuează crearea şi/sau expedierea documentului electronic şi în documentul electronic se conţine informaţia care identifică persoana în numele căreia a fost creat şi expediat documentul electronic.

(2) Actele normative şi/sau acordul părţilor, care stabilesc cazurile de recunoaştere a documentelor electronice semnate cu semnătura electronică simplă, echivalente documentelor pe suport de hîrtie semnate cu semnătura olografă, trebuie să prevadă următoarele:

a) modalitatea de identificare a persoanei în numele căreia este semnat documentul electronic în baza semnăturii electronice simple a acesteia;

b) obligaţia persoanei care creează şi/sau utilizează date de creare a semnăturii electronice simple de a asigura confidenţialitatea acestora.

Articolul 11. Limitele utilizării unor tipuri de semnături electronice

(1) Nu se admite utilizarea semnăturii electronice simple şi a semnăturii electronice avansate necalificate pentru:

a) semnarea documentelor electronice ce conţin informaţie atribuită la secretul de stat;

b) semnarea documentelor electronice în raporturile juridice ale persoanelor juridice de drept public cu persoanele fizice şi cu persoanele juridice de drept privat.

(2) Prin derogare de la prevederile alin. (1) lit. a), se admite semnarea documentelor electronice ce conţin informaţie atribuită la secret de stat, cu semnătura electronică avansată necalificată, de către persoanele ale căror identitate și calitate constituie secret de stat, în condițiile Legii nr. 245/2008 cu privire la secretul de stat, din cadrul Serviciului de Informații și Securitate, Centrului Național Anticorupție și Ministerului Afacerilor Interne, la circulația electronică a documentelor din cadrul acestora.

[Art.11 al.(2) introdus prin LP317 din 30.11.18, MO1-5/04.01.19 art.40; în vigoare 04.02.19; alineatul unic devine alineatul (1)]

Articolul 12. Registrul împuternicirilor de reprezentare în baza semnăturii electronice

(1) Registrul împuternicirilor de reprezentare în baza semnăturii

electronice conţine date privind persoanele împuternicite, persoanele reprezentate, rolul şi scopul împuternicirilor, data acordării împuternicirilor, durata împuternicirilor, alte menţiuni privind acordarea, modificarea sau retragerea împuternicirilor. Împuternicirile pentru care este necesară forma autentică sînt înregistrate în Registrul împuternicirilor de reprezentare în baza semnăturii electronice cu respectarea legislaţiei notariale.

(2) Orice modificare în Registrul împuternicirilor de reprezentare în baza semnăturii electronice privind delegarea împuternicirilor poate fi realizată doar de către persoana care acordă împuternicirile respective.

(3) Posesorul şi deţinătorul Registrului împuternicirilor de reprezentare în baza semnăturii electronice, precum şi modul de creare şi actualizare a acestuia sînt stabilite de Guvern.

Capitolul III
REGIMUL JURIDIC AL DOCUMENTULUI ELECTRONIC ŞI CIRCULAŢIA ELECTRONICĂ A DOCUMENTELOR

Articolul 13. Regimul juridic de utilizare a documentului electronic

(1) Documentul electronic semnat cu semnătură electronică avansată calificată este asimilat, după efectele sale, cu documentul analog pe suport de hîrtie, semnat cu semnătură olografă.

(2) Documentul electronic semnat cu semnătură electronică simplă sau cu semnătură electronică avansată necalificată este asimilat, după efectele sale, cu documentul analog pe suport de hîrtie, semnat cu semnătură olografă, doar în cazurile stabilite expres de actele normative sau de acordul părţilor privind aplicarea semnăturilor electronice, cu respectarea condiţiilor stipulate la art.16 alin.(1).

(3) Actele normative sau acordul părţilor privind aplicarea semnăturilor electronice care stabilesc cazurile de recunoaştere a documentelor electronice, semnate cu semnătură electronică simplă sau cu semnătură electronică avansată necalificată, asimilate, după efectele lor, cu documente analoage pe suport de hîrtie, semnate cu semnătură olografă, trebuie să prevadă modalitatea de verificare a semnăturii electronice, precum şi obligaţiile părţilor privind confidenţialitatea şi răspunderea materială.

(4) În cazul în care, conform legislaţiei, se cere ca documentul să fie perfectat sau prezentat pe suport de hîrtie şi semnat cu semnătură olografă, documentul electronic se consideră a fi corespunzător acestei cerinţe.

(5) În cazul în care, conform legislaţiei, se cere ca documentul pe suport de hîrtie să fie autentificat cu ştampilă, documentul electronic se consideră a fi corespunzător acestei cerinţe.

(6) Cu o singură semnătură electronică pot fi semnate cîteva documente electronice legate între ele (setul de documente electronice). În cazul semnării cu semnătură electronică a setului de documente electronice, fiecare document inclus în acest set se consideră semnat cu acelaşi tip de semnătură electronică.

(7) Modul de utilizare a documentelor electronice în cadrul procedurilor judiciare este reglementat de legislaţia procesuală.

(8) Documentul electronic este echivalat, după valoarea sa probantă, cu probele scrise sau mijloacele materiale de probă. Documentul electronic nu poate fi respins în calitate de probă pentru motivul că are o formă electronică.

(9) În cazul în care legislaţia prevede înregistrarea de stat a documentului, documentul electronic se supune înregistrării.

(10) Toate exemplarele identice ale documentului electronic sînt considerate originale şi produc aceleaşi efecte juridice.

(11) În cazul în care o persoană creează un document electronic şi un document pe suport de hîrtie, identice după conţinut, ambele se consideră documente de sine stătătoare şi originale.

(12) Copie a documentului electronic se consideră reprezentarea (redarea) acestuia pe suport de hîrtie, într-o formă perceptibilă. Copia documentului electronic se autentifică în modul prevăzut de legislaţie pentru autentificarea copiilor documentelor pe suport de hîrtie şi conţine menţiunea despre faptul că este copie a documentului electronic.

Articolul 14. Domeniile şi scopul de utilizare a documentului electronic

(1) Documentul electronic poate fi utilizat de către persoanele fizice şi juridice în toate domeniile de activitate în care este posibilă utilizarea mijloacelor tehnice şi de program ce permit crearea, prelucrarea, expedierea, recepţionarea, păstrarea, modificarea şi/sau nimicirea informaţiei în formă electronică.

(2) Documentul electronic poate fi utilizat în scopul expedierii informaţiei, ţinerii corespondenţei, întocmirii actelor juridice, precum şi în calitate de document care reflectă fapte economice.

Articolul 15. Cerinţele faţă de documentul electronic

Documentul electronic trebuie să corespundă următoarelor cerinţe principale:

a) să fie creat, prelucrat, expediat, recepţionat, păstrat, modificat şi/sau nimicit cu ajutorul mijloacelor tehnice şi/sau de program;

b) să conţină, pentru confirmarea autenticităţii acestuia, una sau mai multe semnături electronice ce corespund condiţiilor şi cerinţelor stabilite de prezenta lege;

c) să fie creat şi utilizat prin metode şi într-o formă ce ar permite identificarea semnatarului;

d) să fie afişat într-o formă perceptibilă;

e) să permită utilizarea sa repetată.

Articolul 16. Autenticitatea documentului electronic

(1) Documentul electronic este considerat autentic dacă întruneşte cumulativ următoarele condiţii:

a) este semnat de persoana abilitată, în modul stabilit, să semneze cu semnătură olografă documentul echivalent pe suport de hîrtie;

b) este semnat cu semnătura electronică autentică a semnatarului indicat în document.

(2) Verificarea autenticităţii documentului electronic se efectuează prin verificarea, cu ajutorul dispozitivelor de verificare a semnăturii electronice şi/sau al produsului asociat semnăturii electronice, a autenticităţii acestei semnături.

Articolul 17. Organizarea circulaţiei electronice a documentelor

(1) Circulaţia electronică a documentelor este organizată conform prevederilor prezentei legi şi regulilor stabilite de către proprietarul sistemului de circulaţie electronică a documentelor, precum şi conform contractelor încheiate între subiecţii circulaţiei electronice a documentelor.

(2) Circulaţia electronică a documentelor poate include:

a) crearea şi prelucrarea documentului electronic;

b) expedierea şi recepţionarea documentului electronic;

c) verificarea autenticităţii documentului electronic;

d) confirmarea recepţionării documentului electronic;

e) evidenţa documentelor electronice;

f) păstrarea, modificarea şi/sau nimicirea documentului electronic;

g) crearea exemplarelor suplimentare ale documentului electronic;

h) crearea şi autentificarea copiilor documentului electronic pe suport de hîrtie;

i) aplicarea mărcii temporale.

(3) Modul de creare, prelucrare, expediere, recepţionare, păstrare, modificare şi/sau nimicire a documentului electronic pentru sistemele de circulaţie electronică a documentelor persoanelor juridice de drept public se stabileşte de Guvern, iar pentru sistemele de circulaţie electronică a documentelor persoanelor juridice de drept privat – de către proprietarii acestora.

Articolul 18. Intermediarul în circulaţia electronică a documentelor

(1) La organizarea şi efectuarea circulaţiei electronice a documentelor pot participa intermediari în condiţiile prezentei legi şi în conformitate cu regulile stabilite de proprietarul sistemului de circulaţie electronică a documentelor.

(2) Intermediarul în circulaţia electronică a documentelor este obligat:

a) să dispună de utilaje şi mijloace tehnice şi/sau de program ce asigură fiabilitatea şi securitatea sistemelor informaţionale utilizate;

b) să dispună de personal cu competenţă şi experienţă în domeniul tehnologiei informaţiei şi/sau al securităţii informaţionale;

c) să asigure condiţiile necesare pentru stabilirea exactă a timpului şi a sursei de expediere a documentului electronic, precum şi a timpului recepţionării şi a adresei electronice a destinatarului;

d) să asigure protecţia şi păstrarea documentelor electronice;

e) să păstreze documentele electronice conform contractului cu utilizatorii sistemului de circulaţie electronică a documentelor.

Articolul 19. Crearea documentului electronic

(1) Documentul electronic este creat de semnatar şi conţine informaţia ce constituie conţinutul documentului electronic şi semnătura electronică a semnatarului.

(2) Crearea documentului electronic se finalizează prin aplicarea semnăturii electronice de către semnatar şi, după caz, prin aplicarea mărcii temporale.

Articolul 20. Expedierea şi recepţionarea documentului electronic

(1) Documentul electronic poate fi expediat şi recepţionat cu ajutorul sistemelor informaţionale şi de comunicaţii electronice şi/sau al purtătorilor materiali.

(2) Documentul electronic se expediază într-o formă ce permite păstrarea şi utilizarea lui de către destinatar.

(3) În cazul în care semnatarul şi destinatarul documentului electronic nu au convenit altfel, documentul electronic se consideră expediat dacă:

a) este expediat de către semnatar ori de către un intermediar în circulaţia electronică a documentelor, care acţionează în numele semnatarului, sau prin sistemul informaţional utilizat de către semnatar;

b) este adresat în mod corespunzător sau este direcţionat în sistemul informaţional indicat de destinatar;

c) este redat într-o formă ce permite prelucrarea lui în sistemul informaţional indicat de destinatar;

d) intră într-un sistem informaţional ce nu este controlat de către semnatar sau de către intermediarul în circulaţia electronică a documentelor care expediază documentul electronic în numele semnatarului.

(4) În cazul în care semnatarul şi destinatarul documentului electronic nu au convenit altfel, documentul electronic se consideră recepţionat de către destinatar dacă acesta:

a) intră în sistemul informaţional din care destinatarul poate să extragă documentele electronice;

b) intră în sistemul informaţional indicat de destinatar într-o formă accesibilă pentru utilizare în sistemul respectiv.

(5) Documentul electronic se consideră neexpediat în cazul în care destinatarul ştia sau trebuia să ştie că:

a) persoana indicată în document ca semnatar nu este semnatarul adevărat al acestuia;

b) semnatarul nu este iniţiatorul expedierii documentului electronic;

c) documentul electronic este recepţionat de către destinatar cu modificări sau fără semnătură electronică.

(6) Documentul electronic nu se consideră recepţionat dacă persoana care l-a recepţionat nu este destinatarul preconizat al acestuia.

Articolul 21. Momentul expedierii şi recepţionării documentului electronic

(1) Dacă semnatarul şi destinatarul documentului electronic nu au convenit altfel, moment al expedierii documentului electronic se consideră

momentul intrării acestuia în sistemul informaţional ce nu este controlat de către semnatar sau de către intermediarul în circulaţia electronică a documentelor care expediază documentul electronic în numele semnatarului.

(2) Dacă semnatarul şi destinatarul documentului electronic nu au convenit altfel, moment al recepţionării documentului electronic se consideră momentul intrării acestuia în sistemul informaţional indicat de destinatar. În cazul în care destinatarul documentului electronic nu a indicat sistemul informaţional respectiv, documentul electronic se consideră recepţionat din momentul intrării acestuia în sistemul informaţional al destinatarului, iar în cazul în care destinatarul nu dispune de un asemenea sistem – din momentul extragerii de către destinatar a documentului electronic din sistemul informaţional prin care a fost transmis.

(3) Momentul expedierii documentului electronic în sistemele informaţionale poate fi confirmat, la necesitate, prin aplicarea mărcii temporale pe documentul electronic respectiv.

(4) Dacă semnatarul şi destinatarul documentului electronic au convenit asupra confirmării recepţionării documentului electronic, moment al recepţionării acestuia se consideră momentul expedierii de către destinatar a confirmării privind recepţionarea, cu aplicarea mărcii temporale după caz.

Articolul 22. Evidenţa documentelor electronice

(1) Evidenţa documentelor electronice ale persoanelor fizice şi/sau juridice se efectuează în conformitate cu legislaţia, prin ţinerea registrelor electronice şi/sau pe suport de hîrtie.

(2) Ţinerea registrelor electronice cuprinde procedurile tehnologice şi de program de completare şi administrare a acestora, precum şi mijloacele de păstrare a documentelor electronice.

Articolul 23. Păstrarea documentelor electronice

(1) Subiecţii circulaţiei electronice a documentelor sînt obligaţi să păstreze originalele documentelor electronice pe suport material într-o formă ce permite verificarea autenticităţii acestora.

(2) Termenul de păstrare a documentelor electronice este identic cu termenul prevăzut de legislaţie pentru păstrarea documentelor echivalente pe suport de hîrtie.

(3) Subiecţii circulaţiei electronice a documentelor pot asigura păstrarea acestora utilizînd serviciile intermediarului în circulaţia electronică a documentelor, cu condiţia respectării prevederilor prezentei legi.

(4) Pentru păstrarea în arhivă a documentelor electronice se utilizează arhiva electronică. Guvernul stabileşte categoriile de documente electronice pentru a căror păstrare se utilizează arhiva electronică securizată.

Articolul 24. Protecţia documentului electronic

(1) Documentul electronic beneficiază de protecţie juridică egală cu cea a documentului analog pe suport de hîrtie.

(2) Informaţia ce constituie conţinutul documentului electronic este utilizată şi protejată, conform legislaţiei, în funcţie de statutul şi gradul de pro-

tecţie a acesteia.

(3) Crearea, prelucrarea, expedierea, recepţionarea, păstrarea, modificarea şi/sau nimicirea documentului electronic trebuie să corespundă cerinţelor de securitate stabilite de Guvern pentru sistemele de circulaţie electronică a documentelor persoanelor juridice de drept public. Cerinţele de securitate pentru sistemele de circulaţie electronică a documentelor persoanelor juridice de drept privat sînt stabilite de către proprietarii acestora.

(4) În procesul de creare, prelucrare, expediere, recepţionare, păstrare, modificare şi/sau nimicire a documentului electronic se impune păstrarea informaţiei ce permite stabilirea originii, apartenenţei şi destinaţiei documentului electronic, precum şi a datei creării, expedierii şi recepţionării acestuia.

Capitolul IV
SERVICIILE DE CERTIFICARE

Articolul 25. Prestatorul de servicii de certificare

(1) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple şi a semnăturii electronice avansate necalificate beneficiază de dreptul de a trece procedura de acreditare. Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate se supun acreditării obligatorii în conformitate cu prevederile prezentei legi.

(2) Prestatorii de servicii de certificare sînt organizaţi în mod ierarhic. În vîrful ierarhiei se află prestatorul de servicii de certificare de nivel superior.

(3) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple şi a semnăturii electronice avansate necalificate îşi organizează ierarhia de sine stătător.

(4) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple formează un singur nivel ierarhic. Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate necalificate formează două niveluri ierarhice, inclusiv superior.

(5) Activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, inclusiv ierarhia acestora, se organizează în modul stabilit de Guvern, în conformitate cu prevederile prezentei legi.

(6) Evidenţa prestatorilor de servicii de certificare acreditaţi se ţine de către organul competent în cadrul Registrului de evidenţă a prestatorilor de servicii de certificare, care se actualizează permanent şi la care accesul este public.

(7) Înregistrarea în Registrul de evidenţă a prestatorilor de servicii de certificare se efectuează de către organul competent la data acreditării acestora.

Articolul 26. Acreditarea prestatorului de servicii de certificare

(1) Acreditarea prestatorului de servicii de certificare se efectuează de către organul competent în baza cererii depuse. Acreditarea prestatorului de servicii de certificare este gratuită şi se acordă pentru un termen de 5 ani, dacă un termen mai mic nu este indicat în cererea de acreditare.

(1[1]) Modul de solicitare, acordare, suspendare şi retragere a certificatului de acreditare a prestatorului de servicii de certificare se stabileşte de Legea nr.160/2011 privind reglementarea prin autorizare a activităţii de întreprinzător în partea în care nu este reglementat de prezenta lege.

(2) Acreditarea în domeniul aplicării semnăturii electronice avansate calificate se acordă prestatorului de servicii de certificare, care întruneşte următoarele cerinţe:

a) dispune de resurse financiare (garanţie bancară sau poliţă de asigurare) în valoare de cel puţin 300 de mii de lei pentru recuperarea unor eventuale prejudicii aduse terţilor din cauza încrederii acestora în datele conţinute în certificatul cheii publice eliberat de către prestatorul de servicii de certificare sau în informaţia din registrul certificatelor eliberate de către prestatorul de servicii de certificare;

b) dispune, pentru prestarea serviciilor de certificare, de personal cu studii superioare în domeniul tehnologiei informaţiei şi/sau al securităţii informaţionale, cu nivel corespunzător de competenţe şi experienţă de gestionare şi expertizare în domeniul tehnologiei semnăturilor electronice;

c) asigură securitatea, fiabilitatea şi continuitatea activităţii de prestare a serviciilor de certificare;

d) asigură înregistrarea informaţiei în registrul certificatelor cheilor publice, în special prestează operativ serviciul de suspendare a valabilităţii certificatului cheii publice şi de revocare a acestuia;

e) asigură posibilitatea de stabilire cu exactitate a datei şi a orei eliberării, suspendării valabilităţii certificatului cheii publice sau revocării acestuia;

f) verifică, în conformitate cu legislaţia, identitatea persoanei pentru care se eliberează un certificat calificat al cheii publice;

g) utilizează sisteme şi produse care sînt protejate împotriva modificărilor şi garantează siguranţa tehnică şi criptografică a funcţiilor pe care şi le asumă;

h) creează condiţii de evitare a falsificării certificatelor şi, în cazul în care prestatorul de servicii de certificare generează date de creare de semnături electronice, garantează confidenţialitatea în procesul de generare a acestor date;

i) utilizează sisteme care nu stochează sau nu copiază datele de creare a semnăturii electronice ale persoanelor pentru care prestatorul de servicii de certificare a prestat servicii de gestionare a cheilor;

j) utilizează sisteme fiabile pentru stocarea certificatelor într-o formă care poate fi verificată, astfel încît:

– numai persoanele autorizate să poată introduce şi modifica date;

– autenticitatea informaţiei să poată fi controlată;

– certificatele să fie disponibile publicului pentru informare;

– toate modificările tehnice care compromit cerinţele de siguranţă să fie vizibile pentru operator.

(3) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate prezintă, pe suport de hîrtie, în format electronic sau prin intermediul ghişeului unic de solicitare a actelor permisive, cererea de acreditare cu anexarea documentelor care confirmă întrunirea cerinţelor specificate la alin.(2) şi, în special, atestă:

a) dispunerea de resurse financiare pentru recuperarea unor eventuale prejudicii;

b) existenţa unei reglementări interne privind asigurarea activităţii prestatorului de servicii de certificare în conformitate cu prevederile prezentei legi;

c) corespunderea sistemelor şi a produselor utilizate cu cerinţele prezentei legi;

d) studiile şi calificările persoanelor cu funcţii de răspundere, ale căror obligaţii funcţionale ţin nemijlocit de prestarea serviciilor de certificare;

e) numirea persoanelor responsabile de activitatea prestatorului de servicii de certificare şi a persoanelor împuternicite să semneze certificatele cheilor publice, precum şi identitatea acestora;

f) ordinea de sincronizare cu Timpul Mondial Coordonat (UTC);

g) dreptul de import, export, proiectare, producere şi comercializare a mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei, precum şi dreptul de prestare a serviciilor în domeniul protecţiei criptografice şi tehnice a informaţiei, cu excepţia activităţii desfăşurate de autorităţile publice învestite cu acest drept prin lege (licenţa).

(4) Documentele menţionate la alin.(3) lit.a) se prezintă în original. Documentele menţionate la alin.(3) lit.b)-g) se prezintă în original, însoţite de cîte o copie, originalul fiind restituit după verificarea copiei la momentul prezentării.

(5) La depunerea cererii de acreditare, prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate este obligat să prezinte, în formatul stabilit de organul competent, informaţiile referitoare la procedurile de securitate şi de certificare utilizate, precum şi datele sale de identificare.

(6) Organul competent, în baza documentelor prezentate şi în termen de 30 de zile calendaristice, adoptă decizia privind acreditarea prestatorului de servicii de certificare sau privind refuzul de acreditare.

(7) În cazul adoptării deciziei de acreditare, organul competent, în termen de 10 zile calendaristice din momentul luării deciziei, notifică prestatorul de servicii de certificare despre decizia luată şi eliberează acestuia certificatul de acreditare de modelul stabilit şi, în conformitate cu actele normative în domeniul semnăturii electronice, înregistrează prestatorul acreditat în Registrul de evidenţă a prestatorilor de servicii de certificare.

(8) În cazul adoptării deciziei privind refuzul de acreditare, organul competent, în termen de 10 zile calendaristice din momentul luării deciziei de

refuz, notifică în scris prestatorul de servicii de certificare despre decizia luată, cu indicarea cauzelor refuzului.

(9) Drept temei pentru refuzul de acreditare serveşte necorespunderea prestatorului de servicii de certificare cerinţelor specificate la alin.(2) sau prezentarea informaţiei neveridice în documentele ce se anexează la cererea de acreditare.

(10) Refuzul de acreditare nu poate împiedica depunerea repetată a documentelor în vederea acreditării după înlăturarea cauzelor care au servit temei pentru refuzul de acreditare.

(11) Decizia privind refuzul de acreditare poate fi contestată în instanţa de judecată în modul stabilit.

(12) Prestatorul de servicii de certificare se consideră acreditat din ziua emiterii certificatului de acreditare.

(13) În caz de deteriorare sau pierdere a certificatului de acreditare, prestatorului de servicii de certificare i se eliberează un duplicat al certificatului în termen de 5 zile lucrătoare, în baza cererii depuse.

(14) Informaţia despre prestatorii de servicii de certificare acreditaţi, precum şi despre cei cu acreditarea retrasă se publică de către organul competent pe pagina sa web oficială.

(15) După primirea certificatului de acreditare pentru prestarea serviciilor de certificare în domeniul aplicării semnăturii electronice avansate calificate, cheia publică a prestatorului de servicii de certificare este certificată de către prestatorul de servicii de certificare de nivel superior în conformitate cu regulamentul aprobat de organul competent.

(16) Acreditarea se consideră acordată sau, după caz, prelungită dacă organul competent nu răspunde solicitantului în termenul prevăzut de lege pentru acordarea sau prelungirea acesteia.

(17) După expirarea termenului de acreditare şi în lipsa unei notificări scrise din partea organului competent, acreditarea se consideră prelungită pentru acelaşi termen.

(18) Prestatorii de servicii de certificare acreditaţi în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate sînt obligaţi să comunice organului competent, cu cel puţin 10 zile calendaristice înainte, orice intenţie de modificare a procedurilor de securitate şi de certificare, cu precizarea datei şi orei la care modificarea intră în vigoare, precum şi să confirme, în decurs de 24 de ore, modificarea efectuată.

(19) În cazurile de urgenţă în care securitatea serviciilor de certificare este afectată, prestatorii de servicii de certificare acreditaţi în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate pot efectua modificări ale procedurilor de securitate şi de certificare, urmînd să comunice, în termen de 24 de ore, organului competent modificările efectuate şi justificarea deciziei luate.

(20) Prestatorul de servicii de certificare acreditat este obligat, pe parcursul întregului termen de acreditare, să asigure respectarea cerinţelor în

conformitate cu care a fost acreditat. În cazul apariţiei circumstanţelor care fac imposibilă asigurarea respectării acestor cerinţe, prestatorul de servicii de certificare urmează să notifice organul competent despre acest fapt în decurs de 24 de ore.

(21) Prestatorul de servicii de certificare de nivel superior în domeniul aplicării semnăturii electronice avansate calificate nu este supus acreditării în conformitate cu prevederile prezentei legi.

Articolul 27. Activitatea prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare:

a) creează şi eliberează certificatele cheilor publice;

b) suspendă şi revocă certificatele cheilor publice, restabileşte valabilitatea certificatelor suspendate;

c) ţine registrul certificatelor cheilor publice, asigură actualizarea acestuia şi accesul public la registru; şi/sau

d) prestează, în bază de contract, alte tipuri de servicii ce ţin de semnătura electronică.

(2) Activitatea prestatorului de servicii de certificare reprezintă o activitate în domeniul protecţiei criptografice şi tehnice a informaţiei şi este supusă licenţierii de către organul de licenţiere în conformitate cu legislaţia în domeniul reglementării prin licenţiere a activităţii de întreprinzător.

Articolul 28. Obligaţiile prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare este obligat:

a) să verifice autenticitatea datelor indicate în cererea de certificare a cheii publice în baza documentelor ce confirmă datele în cauză;

b) să asigure corespunderea informaţiilor din certificatul cheii publice cu informaţiile prezentate de către titularul certificatului cheii publice;

c) să introducă certificatul cheii publice în registrul certificatelor cheilor publice nu mai tîrziu de data şi ora la care începe să curgă termenul de valabilitate a certificatului;

d) să asigure accesul la registrul certificatelor cheilor publice, cu respectarea prevederilor art.43;

e) să suspende valabilitatea sau să revoce certificatul cheii publice în cazurile prevăzute de lege şi să facă menţiunea respectivă în registrul certificatelor cheilor publice în termenele stabilite;

f) să acopere prejudiciile aduse oricărei entităţi sau persoane fizice, care se încrede în mod rezonabil în datele conţinute în certificatul cheii publice eliberat de către prestatorul de servicii de certificare, prin faptul că a omis să înregistreze revocarea certificatului;

g) să înştiinţeze titularul certificatului cheii publice despre faptele care au devenit cunoscute prestatorului de servicii de certificare şi care fac imposibilă utilizarea în continuare a cheii private, precum şi despre revocarea certificatului cheii publice;

h) să prezinte informaţiile necesare pentru autentificarea semnăturii electronice;

i) să solicite eliberarea duplicatului certificatului de acreditare în cazul pierderii sau deteriorării acestuia;

j) să îndeplinească alte obligaţii stabilite de prezenta lege.

(2) Prestatorul de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate este obligat, suplimentar:

a) să certifice, în modul stabilit de legislaţie, cheia publică a prestatorului de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate, destinată certificării cheilor publice;

b) să înregistreze, pe o perioadă stabilită de timp, în conformitate cu art.31, toate informaţiile pertinente referitoare la un certificat calificat al cheii publice, în special pentru a putea furniza dovezi privind certificarea în justiţie. Înregistrările pot fi efectuate prin mijloace electronice;

c) înainte să stabilească o relaţie contractuală cu o persoană care solicită un certificat în sprijinul semnăturii sale electronice, să informeze respectiva persoană, prin mijloace de comunicare fiabile, cu privire la termenele şi condiţiile exacte de utilizare a certificatului, inclusiv cu privire la limitele impuse utilizării acestui certificat, la existenţa unui sistem de acreditare şi la procedurile de contestare şi soluţionare a litigiilor. Aceste informaţii, care pot fi transmise pe cale electronică, trebuie comunicate în scris, într-un limbaj accesibil. Elementele pertinente ale informaţiilor trebuie puse, de asemenea, la cerere, la dispoziţia părţilor terţe care beneficiază de certificat;

d) să păstreze toată informaţia cu privire la certificatul cheii publice ataşat semnăturilor electronice avansate calificate cel puţin 15 ani de la data revocării sau expirării certificatului, în eventualitatea unor litigii.

Articolul 29. Cererea de certificare a cheii publice

(1) Cererea de certificare a cheii publice se depune în formă electronică semnată cu semnătură electronică şi/sau în formă de document pe suport de hîrtie, semnat cu semnătura ologrfă a solicitantului.

(2) Cererea de certificare a cheii publice va conţine:

a) numele şi prenumele solicitantului şi numărul actului de identitate;

b) alte date de identificare ale solicitantului, în funcţie de scopul pentru care se eliberează certificatul cheii publice, precum şi informaţiile necesare pentru comunicarea cu acesta.

Articolul 30. Examinarea cererii de certificare a cheii publice

(1) Cererea de certificare a cheii publice este examinată de către prestatorul de servicii de certificare în termen de 3 zile lucrătoare de la data înregistrării cererii, dacă părţile nu stabilesc altfel.

(2) În baza deciziei de certificare a cheii publice, prestatorul de servicii de certificare creează şi eliberează certificatul cheii publice.

(3) Decizia privind refuzul de certificare a cheii publice se adoptă de către prestatorul de servicii de certificare în cazul:

a) încălcării prevederilor prezentei legi;

b) încălcării drepturilor unor terţi în procesul de întocmire sau de depunere a cererii de certificare;

c) prezentării în cererea de certificare a unor informaţii ce nu corespund realităţii.

(4) Decizia privind refuzul de certificare a cheii publice poate fi contestată în instanţa de judecată în modul stabilit.

(5) Decizia privind refuzul de certificare a cheii publice nu-l privează pe solicitant de dreptul de a depune o nouă cerere după înlăturarea tuturor încălcărilor admise.

Articolul 31. Certificatul cheii publice

(1) La crearea certificatului cheii publice, prestatorul de servicii de certificare este obligat să verifice unicitatea cheii publice.

(2) Certificatul cheii publice trebuie să conţină:

a) numărul unic de înregistrare a certificatului cheii publice;

b) datele de identificare ale prestatorului de servicii de certificare care a eliberat certificatul cheii publice;

c) datele de identificare şi alte date ale titularului certificatului cheii publice, în funcţie de scopul pentru care se eliberează certificatul, precum şi informaţiile necesare pentru comunicarea cu acesta;

d) cheia publică;

e) data şi ora la care începe să curgă termenul de valabilitate a certificatului cheii publice şi data şi ora la care acest termen încetează;

f) date despre algoritmul criptografic al semnăturii electronice;

g) restricţiile privind utilizarea certificatului cheii publice şi/sau limitele valorii operaţiunilor în care acesta poate fi utilizat, dacă acestea se aplică;

h) alte informaţii prevăzute de legislaţie.

(3) Certificatul calificat al cheii publice se emite de către prestatorul de servicii de certificare acreditat şi trebuie să conţină, suplimentar:

a) menţiunea care să indice că certificatul este eliberat ca certificat calificat al cheii publice;

b) informaţia, atunci cînd este cazul, privind o calitate specială a semnatarului, în funcţie de utilizarea pe care urmează să o aibă certificatul;

c) datele de verificare a semnăturii electronice care corespund datelor de creare a semnăturii electronice controlate de semnatar.

(4) Date de identificare ale titularului, în cazul certificatului cheii publice al utilizatorului, se consideră numele, prenumele şi numărul de identificare a persoanei fizice (IDNP) şi/sau pseudonimul, dacă există, iar în cazul certificatului cheii publice al prestatorului de servicii de certificare – denumirea prestatorului şi numărul de identificare a persoanei juridice (IDNO).

(5) În cazul semnăturii electronice simple şi al semnăturii electronice avansate necalificate, structura certificatului cheii publice se stabileşte de către prestatorul de servicii de certificare, în conformitate cu prevederile prezentei legi. În cazul semnăturii electronice avansate calificate, structura certificatului cheii publice se stabileşte de către organul competent, în conformitate cu prevederile prezentei legi.

(6) Certificatul cheii publice se semnează cu semnătura electronică a

prestatorului de servicii de certificare corespunzătoare tipului certificatului solicitat.

(7) În cazurile stabilite de legislaţie sau prin acordul părţilor, prestatorul de servicii de certificare creează certificatul cheii publice şi în formă de document pe suport de hîrtie, în două exemplare. Certificatul cheii publice în formă de document pe suport de hîrtie este semnat cu semnăturile olografe ale titularului certificatului cheii publice şi ale persoanei împuternicite a prestatorului de servicii de certificare şi este autentificat cu ştampila prestatorului de servicii de certificare. Un exemplar al certificatului cheii publice se transmite titularului, iar celălalt se păstrează la prestatorul de servicii de certificare.

(8) Prestatorul de servicii de certificare, de comun acord cu titularul certificatului cheii publice, poate indica în certificatul cheii publice cazurile în care certificatul respectiv va putea fi utilizat, precum şi unele restricţii cu privire la utilizarea acestuia.

(9) La cererea titularului certificatului cheii publice, prestatorul de servicii de certificare poate indica în certificatul cheii publice şi alte informaţii decît cele specificate la alin.(2) şi (3), cu condiţia că acestea nu contravin legislaţiei şi nu pun în pericol securitatea naţională sau ordinea publică, şi numai după o prealabilă verificare a exactităţii informaţiilor în cauză.

(10) Prestatorul de servicii de certificare introduce certificatul în registrul certificatelor cheilor publice nu mai tîrziu de data şi ora la care începe să curgă termenul de valabilitate a certificatului.

Articolul 32. Termenul de valabilitate şi termenul de păstrare a certificatului cheii publice

(1) Termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de certificare de nivel superior constituie 20 de ani, termenul de valabilitate a certificatului cheii publice al prestatorului de servicii de certificare de nivelul II constituie 10 ani, termenul de valabilitate a certificatului cheii publice al utilizatorului se stabileşte de către prestatorul de servicii de certificare, dar nu poate constitui mai mult de 5 ani, în funcţie de capacităţile mijloacelor tehnice de creare a semnăturii electronice.

(2) Prestatorul de servicii de certificare este obligat să păstreze certificatul cheii publice cel puţin 15 ani de la data revocării sau expirării certificatului.

Articolul 33. Suspendarea şi revocarea certificatului cheii publice

(1) Prestatorul de servicii de certificare suspendă certificatul cheii publice la cererea titularului certificatului cheii publice.

(2) Prestatorul de servicii de certificare revocă certificatul cheii publice:

a) la cererea titularului certificatului cheii publice;

b) la depistarea unor informaţii neveridice în cererea de certificare a cheii publice sau în certificatul cheii publice;

c) la încălcarea confidenţialităţii cheii private (compromiterea cheii private);

d) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice şi în lipsa unei cereri din partea titularului certificatului cheii publice privind restabilirea valabilităţii acestuia;

e) la modificarea certificatului cheii publice;

f) în cazul decesului titularului certificatului cheii publice sau al instituirii unei măsuri de ocrotire judiciare (ocrotire provizorie, curatelă sau tutelă) în privinţa titularului;

g) la solicitarea organului competent, în cazul încălcării prezentei legi.

(3) În cazul în care prestatorul de servicii de certificare primeşte informaţii ce impun revocarea certificatului cheii publice, acesta este obligat, în termen de 3 ore de lucru, să facă menţiunile respective în registrul certificatelor cheilor publice.

(4) Prestatorul de servicii de certificare este obligat să înştiinţeze titularul certificatului cheii publice despre motivele revocării certificatului acestuia.

Articolul 34. Obligaţiile titularului certificatului cheii publice

Titularul certificatului cheii publice este obligat:

a) să asigure condiţiile necesare pentru excluderea accesului unei alte persoane la cheia sa privată;

b) să nu utilizeze cheia privată pentru crearea semnăturii electronice dacă are motive să presupună că este încălcată confidenţialitatea cheii private;

c) să solicite imediat suspendarea valabilităţii certificatului cheii publice sau revocarea acestuia în cazul în care:

– a pierdut cheia privată;

– are motive să creadă că a fost încălcată confidenţialitatea cheii private;

– informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;

d) să înştiinţeze, în decurs de 24 de ore, prestatorul de servicii de certificare despre orice modificare a informaţiilor cuprinse în certificatul cheii publice;

e) să îndeplinească alte obligaţii prevăzute de prezenta lege şi de acordul încheiat cu prestatorul de servicii de certificare.

Articolul 35. Registrul certificatelor cheilor publice

(1) Prestatorul de servicii de certificare este obligat să ţină registrul certificatelor cheilor publice.

(2) Registrul certificatelor cheilor publice va conţine:

a) certificatele valabile ale cheilor publice;

b) certificatele revocate şi suspendate ale cheilor publice;

c) data şi ora eliberării certificatelor cheilor publice;

d) data şi ora revocării certificatelor cheilor publice;

e) alte informaţii în conformitate cu actele normative în domeniul semnăturii electronice.

(3) În vederea verificării autenticităţii semnăturii electronice, prestatorul de servicii de certificare este obligat să asigure accesul la registrul certifica-

telor cheilor publice, inclusiv în regimul timpului real.

Capitolul V
MONITORIZARE ŞI CONTROL

Articolul 36. Atribuţiile autorităţilor publice în domeniul aplicării semnăturii electronice

(1) Organul competent responsabil de elaborarea şi promovarea politicii de stat şi de exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice este Serviciul de Informaţii şi Securitate, care exercită următoarele atribuţii:

a) efectuează acreditarea, inclusiv voluntară, a prestatorilor de servicii de certificare;

b) exercită funcţia prestatorului de servicii de certificare de nivel superior pentru prestatorii de servicii de certificare acreditaţi în domeniul aplicării semnăturii electronice avansate calificate;

c) asigură ţinerea, actualizarea şi accesul public la datele Registrului de evidenţă a prestatorilor de servicii de certificare;

d) elaborează şi aprobă, prin acte normative, cerinţele în domeniul aplicării tuturor tipurilor de semnături electronice;

e) monitorizează şi controlează respectarea cerinţelor la prestarea serviciilor de certificare în domeniul aplicării tuturor tipurilor de semnături electronice;

f) participă la elaborarea şi aprobarea reglementărilor tehnice şi a standardelor în domeniul semnăturii electronice;

g) acordă, la solicitare, asistenţă metodică şi practică la aplicarea mecanismelor semnăturii electronice;

h) realizează colaborarea internaţională în domeniul semnăturii electronice.

(2) Guvernul stabileşte autoritatea sau instituţia publică responsabilă de prestarea serviciului de sursă unică de sincronizare cu Timpul Mondial Coordonat (UTC).

Articolul 37. Controlul în domeniul aplicării semnăturii electronice

(1) Organul competent controlează respectarea cerinţelor stabilite de prezenta lege la prestarea serviciilor de certificare de către prestatorii acreditaţi şi la acordarea sau prelungirea acreditării.

(2) Controlul se efectuează de către comisia de control în domeniul semnăturii electronice (în continuare – Comisia) în baza regulamentului aprobat de organul competent.

(3) Comisia se creează în cadrul organului competent în baza ordinului privind efectuarea controlului, emis de conducătorul acestui organ.

(4) Componenţa nominală a Comisiei se stabileşte pentru fiecare caz în parte.

(5) Comisia are dreptul:

a) să beneficieze de acces liber la materialele documentare, pe suport

de hîrtie şi în format electronic, necesare pentru desfăşurarea lucrărilor ce ţin de prestarea serviciilor de certificare, precum şi la sistemele de distribuţie de aplicaţii soft, la aplicaţiile soft şi mijloacele tehnice instalate;

b) să obţină informaţii complete despre condiţiile şi modul de exploatare a mijloacelor tehnice şi de program;

c) să obţină de la persoanele responsabile şi de la personalul prestatorului de servicii de certificare informaţiile privind prestarea serviciilor de certificare ce ţin de obiectul controlului;

d) să beneficieze de acces, în decursul zilei lucrătoare (în perioada efectuării controlului), în încăperile prestatorului de servicii de certificare.

(6) Comisia nu are dreptul să efectueze controlul fără prezentarea ordinului privind efectuarea controlului şi fără prezentarea actelor de identitate ale membrilor Comisiei.

(7) La efectuarea controlului privind respectarea condiţiilor prevăzute de prezenta lege, Comisia va ţine cont de următoarele principii:

a) legalitatea şi respectarea competenţei stabilite de lege;

b) neadmiterea aplicării sancţiunilor care nu sînt stabilite de lege;

c) tratarea dubiilor, apărute la aplicarea legislaţiei, în favoarea prestatorului de servicii de certificare;

d) efectuarea controlului pe cheltuiala statului;

e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului;

f) dreptul prestatorului de servicii de certificare de a contesta acţiunile organului competent, inclusiv în instanţa judecătorească.

(8) Controalele planificate privind respectarea de către prestatorul de servicii de certificare a obligaţiilor prevăzute de prezenta lege se efectuează de către organul competent cel mult o dată în decursul anului calendaristic, cu cooptarea, după caz, a reprezentanţilor instituţiilor cu funcţii de reglementare şi de control, conform competenţei.

(9) Planurile controalelor, elaborate de organul competent şi aprobate în modul stabilit, se coordonează, în privinţa termenelor de efectuare, cu conducerea prestatorului de servicii de certificare, cu cel puţin 5 zile lucrătoare înainte de începerea acestor controale.

(10) Controalele inopinate se efectuează la decizia organului competent, numai în temeiul:

a) depistării şi confirmării, de către organul competent, a faptelor de încălcare a prezentei legi; şi/sau

b) recepţionării cererilor şi reclamaţiilor argumentate adresate în formă scrisă organului competent referitoare la încălcările şi la îndeplinirea necorespunzătoare a obligaţiilor prevăzute de prezenta lege de către prestatorul de servicii de certificare.

(11) Prestatorul de servicii de certificare este informat despre efectuarea controlului inopinat în ziua demarării controlului.

(12) Controalele repetate se efectuează numai în scopul verificării exe-

cutării prescripţiei privind lichidarea încălcărilor prezentei legi, indicate în actul de control precedent (planificat sau inopinat). Controlul repetat se consideră parte componentă a controlului precedent.

(13) Controlul se efectuează strict în termenele stabilite în ordinul privind efectuarea controlului.

(14) Termenul de efectuare a controlului planificat şi a controlului inopinat nu poate depăşi 10 zile lucrătoare, iar a celui repetat – 5 zile lucrătoare. În cazul controalelor inopinate, termenul de 10 zile poate fi prelungit cu încă 10 zile de către conducătorul organului competent în baza unei decizii motivate, adusă la cunoştinţa prestatorului de servicii de certificare supus controlului, care poate fi contestată de către prestatorul de servicii de certificare.

(15) La efectuarea controlului privind respectarea obligaţiilor prevăzute de prezenta lege, prestatorul de servicii de certificare prezintă informaţia şi documentele relevante scopului controlului şi nu împiedică efectuarea acestuia.

(16) În baza rezultatelor controlului se întocmeşte un act în 2 exemplare, unul dintre care se expediază/înmînează, în termen de cel mult 5 zile lucrătoare după încheierea controlului efectuat, prestatorului de servicii de certificare, iar al doilea se păstrează la organul competent. În cazul în care nu este de acord cu rezultatele controlului efectuat, prestatorul de servicii de certificare, în termen de 10 zile lucrătoare de la data primirii actului de control, poate prezenta în scris argumentarea dezacordului, anexînd documentele de rigoare.

(17) În cazul în care se depistează încălcări ale obligaţiilor prevăzute de prezenta lege, organul competent emite, în baza actului de control, prescripţia privind lichidarea acestor încălcări, ce cuprinde recomandările privind modul de remediere a tuturor încălcărilor depistate, precum şi avertizarea despre posibila suspendare sau retragere a acreditării dacă acestea nu vor fi lichidate în termenul stabilit.

(18) Termenul minim stabilit de organul competent pentru lichidarea încălcărilor depistate constituie 10 zile lucrătoare, iar cel maxim – 30 de zile lucrătoare după primirea prescripţiei expediate/înmînate împreună cu actul de control.

(19) În cazuri excepţionale şi la solicitarea oficială a prestatorului de servicii de certificare, termenul pentru lichidarea încălcărilor poate fi prelungit cu cel mult 20 de zile lucrătoare.

(20) Prestatorul de servicii de certificare acreditat care a primit prescripţia privind lichidarea încălcărilor obligaţiilor prevăzute de prezenta lege este obligat, în termenul indicat în prescripţie, să comunice organului competent informaţia privind lichidarea încălcărilor.

(21) În cazul constatării semnelor de compromitere a cheilor private ale prestatorului de servicii de certificare acreditat, în cazul încălcării obligaţiilor prevăzute de prezenta lege, precum şi în cazul neînlăturării, în termenul stabilit, a datelor eronate din certificatele cheilor publice, organul competent

poate aplica măsuri de suspendare sau retragere a acreditării prestatorului de servicii de certificare în conformitate cu prezenta lege.

(22) Informaţiile despre rezultatele efectuării controlului se publică de către organul competent pe pagina sa web oficială.

(23) Prestatorul de servicii de certificare are dreptul să depună la organul competent reclamaţii în scris privind încălcările prevederilor prezentei legi admise de Comisie sau să conteste acţiunile acesteia în instanţa judecătorească.

Articolul 38. Suspendarea şi reluarea valabilităţii acreditării

(1) Acreditarea poate fi suspendată în conformitate cu legislaţia în domeniul reglementării activităţii de întreprinzător.

(2) Drept temei pentru realizarea acţiunilor prevăzute de lege pentru suspendarea acreditării servesc:

a) cererea prestatorului de servicii de certificare privind suspendarea acreditării;

b) încălcarea de către prestatorul de servicii de certificare a obligaţiilor stabilite de prezenta lege;

c) nevalabilitatea garanţiei bancare sau a poliţei de asigurare pentru prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, prevăzută la art.26 alin.(2) lit.a);

d) nerespectarea de către prestatorul de servicii de certificare a prescripţiei privind lichidarea încălcărilor obligaţiilor prevăzute de prezenta lege, depistate în urma controlului efectuat de Comisie.

(3) Decizia privind suspendarea acreditării se aduce la cunoştinţă prestatorului de servicii de certificare în termen de 3 zile lucrătoare de la data adoptării acesteia. Termenul de suspendare a acreditării nu poate depăşi 2 luni, dacă actele normative în domeniul semnăturii electronice nu prevăd altfel.

(4) Prestatorul de servicii de certificare este obligat să înştiinţeze în scris organul competent despre înlăturarea circumstanţelor care au dus la suspendarea acreditării.

(5) Decizia privind reluarea valabilităţii acreditării se adoptă de către organul competent în temeiul hotărîrii instanţei de judecată care a emis hotărîrea de suspendare a acreditării, în termen de 3 zile lucrătoare de la data primirii înştiinţării. Decizia se aduce la cunoştinţă prestatorului de servicii de certificare în termen de 3 zile lucrătoare de la data adoptării acesteia.

(6) Termenul de valabilitate a acreditării nu se prelungeşte pe perioada de suspendare a acesteia.

Articolul 39. Retragerea acreditării

(1) Acreditarea poate fi retrasă în conformitate cu legislaţia în domeniul reglementării activităţii de întreprinzător.

(2) Drept temei pentru realizarea acţiunilor prevăzute de lege în vederea retragerii acreditării servesc:

a) cererea prestatorului de servicii de certificare privind încetarea activităţii, depusă cu 30 de zile calendaristice înainte de încetarea planificată;

b) decizia cu privire la anularea înregistrării de stat a persoanei juridice în cadrul căreia activează prestatorul de servicii de certificare;

c) depistarea unor date neautentice în documentele prezentate organului competent;

d) constatarea faptului de transmitere a certificatului de acreditare sau a copiei de pe acesta altei persoane în scopul desfăşurării genului de activitate acreditat;

e) neînlăturarea, în termenul stabilit, a circumstanţelor care au dus la suspendarea acreditării;

f) nerespectarea repetată a prescripţiilor privind lichidarea încălcărilor obligaţiilor stabilite de prezenta lege.

(3) Menţiunea referitoare la data şi numărul deciziei privind retragerea acreditării se înscrie în Registrul de evidenţă a prestatorilor de servicii de certificare nu mai tîrziu de ziua lucrătoare imediat următoare zilei adoptării deciziei.

(4) Toate certificatele cheilor publice emise de către prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate care şi-a încetat activitatea se revocă şi se transmit spre păstrare altui prestator de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, în modul stabilit de organul competent, pe cheltuiala prestatorului de servicii de certificare care îşi încetează activitatea.

(5) Prestatorul de servicii de certificare este obligat, în decurs de 10 zile lucrătoare de la data adoptării deciziei de retragere a acreditării, să depună la organul competent certificatul de acreditare retras.

Capitolul VI
RĂSPUNDEREA

Articolul 40. Răspunderea persoanelor fizice şi juridice care cad sub incidenţa prezentei legi

(1) Persoanele fizice şi juridice poartă răspundere, conform legislaţiei, pentru neîndeplinirea prevederilor prezentei legi.

(2) Intermediarul în circulaţia electronică a documentelor poartă răspundere, conform legislaţiei, pentru neîndeplinirea sau îndeplinirea defectuoasă a obligaţiilor prevăzute de prezenta lege, pentru calitatea necorespunzătoare a serviciilor prestate, precum şi pentru prejudiciul cauzat de aceste acţiuni şi/sau inacţiuni.

(3) Pentru acces ilegal la informaţia cuprinsă în documentele electronice, persoanele poartă răspundere civilă, contravenţională sau penală, după caz, conform legislaţiei.

(4) Litigiile apărute în cadrul circulaţiei electronice a documentelor, precum şi cele legate de utilizarea documentelor electronice şi de aplicarea semnăturii electronice se soluţionează de către subiecţii circulaţiei electronice a documentelor în conformitate cu legislaţia şi contractele încheiate.

Articolul 41. Răspunderea prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare poartă răspundere civilă, contravenţională sau penală, după caz, conform legislaţiei.

(2) Prestatorul de servicii de certificare poartă răspundere civilă pentru prejudiciul cauzat urmare a neîndeplinirii obligaţiilor prevăzute de prezenta lege, cu excepţia cazurilor în care prestatorul de servicii de certificare aduce probe pertinente că nu a putut împiedica cauzarea prejudiciului.

(3) Prestatorul de servicii de certificare nu poartă răspundere civilă pentru prejudiciul cauzat urmare a utilizării certificatului cheii publice cu încălcarea restricţiilor de utilizare a acestuia sau a restricţiilor privind limitele valorii operaţiunilor în care acesta poate fi utilizat.

Articolul 42. Răspunderea titularului certificatului cheii publice

(1) Titularul certificatului cheii publice poartă răspundere civilă, contravenţională sau penală, după caz, conform legislaţiei.

(2) Titularul certificatului cheii publice poartă răspundere civilă pentru prejudiciul cauzat de:

a) neîndeplinirea sau îndeplinirea defectuoasă a obligaţiilor prevăzute de prezenta lege;

b) semnarea documentelor electronice cu utilizarea cheii private, inclusiv în perioada de la solicitarea suspendării valabilităţii sau revocării certificatului cheii publice pînă la înscrierea, în termenul stabilit, a menţiunii respective în registrul certificatelor cheilor publice, cu excepţia cazurilor în care titularul certificatului va aduce probe pertinente că documentul electronic a fost semnat de o altă persoană.

Capitolul VII
PROTECŢIA DATELOR CU CARACTER PERSONAL

Articolul 43. Protecţia datelor cu caracter personal

(1) Prestatorii de servicii de certificare vor asigura respectarea legislaţiei în domeniul protecţiei datelor cu caracter personal în procesul de prestare a serviciilor de certificare.

(2) Datele cu caracter personal se colectează de către prestatorul de servicii de certificare numai cu acordul prealabil al persoanei care solicită certificatul şi numai în măsura în care acestea sînt necesare pentru eliberarea şi menţinerea certificatului. Datele personale nu pot fi colectate sau prelucrate în alte scopuri fără consimţămîntul expres al persoanei interesate.

PARLAMENTUL

COD *Nr. 218 din 24-10-2008*

CODUL CONTRAVENȚIONAL AL REPUBLICII MOLDOVA*

Publicat : 17-03-2017 în Monitorul Oficial Nr. 78-84 art. 100

MODIFICATLP116 din 09.07.20, MO193/27.07.20, art.372; în vigoare 27.07.20

Capitolul II

CONTRAVENȚIA. RĂSPUNDEREA CONTRAVENȚIONALĂ

Articolul 10. Contravenţia

Constituie contravenţie fapta – acţiunea sau inacţiunea – ilicită, cu un grad de pericol social mai redus decît infracţiunea, săvîrşită cu vinovăţie, care atentează la valorile sociale ocrotite de lege, este prevăzută de prezentul cod şi este pasibilă de sancţiune contravenţională.

Titlul II

PARTEA SPECIALĂ

Capitolul VI

CONTRAVENȚII CE ATENTEAZĂ LA DREPTURILE POLITICE, DE MUNCĂ ŞI LA ALTE DREPTURI CONSTITUȚIONALE ALE PERSOANEI FIZICE

Articolul 70. Calomnia

(1) Calomnia, adică răspîndirea cu bună ştiinţă a unor informaţii mincinoase ce defăimează o altă persoană,

se sancţionează cu amendă de la 48 la 72 de unităţi convenţionale aplicată persoanei fizice sau cu muncă neremunerată în folosul comunităţii de la 20 la 60 de ore, cu amendă de la 72 la 150 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere cu privarea de dreptul de a deţine anumite funcţii sau de dreptul de a desfăşura anumite activităţi pe un termen de la 3 luni la un an.

(2) Aceeaşi acţiune însoţită de învinuirea în săvîrşirea unei infracţiuni

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice sau cu muncă neremunerată în folosul comunităţii de la 40 la 60 de ore, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere cu privarea de dreptul de a deţine anumite funcţii sau de dreptul de a desfăşura anumite activităţi pe un termen de la 6 luni la un an.

Articolul 71. Încălcarea legislaţiei privind accesul la informaţie şi cu privire la petiţionare

(1) Încălcarea intenţionată a dispoziţiilor legale privind accesul la informaţie sau a celor cu privire la petiţionare

se sancţionează cu amendă de la 9 la 15 unităţi convenţionale aplicată persoanei fizice, cu amendă de la 18 la 30 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere.

(2) Prezentarea, la solicitare, a unui răspuns cu date vădit eronate

se sancţionează cu amendă de la 27 la 33 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere.

Articolul 74[1]. Prelucrarea datelor cu caracter personal cu încălcarea legislaţiei privind protecţia datelor cu caracter personal

(1) Nerespectarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea lor în cadrul sistemelor informaţionale de date cu caracter personal

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 300 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile, de dreptul de a desfăşura o anumită activitate pe un termen de la 3 luni la un an.

(2) Prelucrarea datelor cu caracter personal fără notificarea şi/sau autorizarea organului de control în domeniul prelucrării datelor cu caracter personal, atunci cînd notificarea sau obţinerea autorizării este obligatorie, precum şi prelucrarea datelor cu caracter personal de un operator neînregistrat în modul stability

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 300 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile,

de dreptul de a desfăşura o anumită activitate pe un termen de la 3 luni la un an.

(3) Încălcarea drepturilor subiectului datelor cu caracter personal de a fi informat, de acces la datele cu caracter personal, de intervenţie asupra datelor cu caracter personal, de opoziţie şi de a nu fi supus unei decizii individuale

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 300 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile, de dreptul de a desfăşura o anumită activitate pe un termen de la 3 luni la un an.

(4) Încălcarea regulilor de prelucrare, stocare şi utilizare a datelor cu caracter personal

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 300 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile, de dreptul de a desfăşura o anumită activitate pe un termen de la 3 luni la un an.

(5) Transmiterea transfrontalieră a datelor cu caracter personal cu încălcarea legislaţiei privind protecţia datelor cu caracter personal

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 300 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile, de dreptul de a desfăşura o anumită activitate pe un termen de la 3 luni la un an.

Articolul 74^2. Refuzul de a furniza informaţii sau împiedicarea accesului personalului Centrului Naţional pentru Protecţia Datelor cu Caracter Personal

(1) Refuzul de a furniza informaţiile sau documentele solicitate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal în procesul exercitării atribuţiilor de control, prezentarea unor informaţii neautentice sau incomplete, precum şi neprezentarea în termenul stabilit de lege a informaţiilor şi a documentelor solicitate

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 60 la 150 de unităţi convenţionale aplicată persoanei juridice.

(2) Împiedicarea accesului personalului abilitat cu funcţii de control al Centrului Naţional pentru Protecţia Datelor cu Caracter Personal în încăperile

şi pe teritoriul amplasării sistemelor de evidenţă a datelor cu caracter personal, la datele cu caracter personal prelucrate de operatori şi/sau de persoanele împuternicite de operatori, la echipamentul de prelucrare, la programe şi aplicaţii, la orice document sau înregistrare referitoare la prelucrarea de date cu caracter personal

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

Articolul 74[3]. Neîndeplinirea deciziilor Centrului Naţional pentru Protecţia Datelor cu Caracter Personal

Neîndeplinirea în termenul stabilit a deciziei Centrului Naţional pentru Protecţia Datelor cu Caracter Personal privind repunerea în drepturi a subiectului datelor cu caracter personal, inclusiv privind suspendarea sau încetarea prelucrării datelor cu caracter personal, privind blocarea, distrugerea parţială ori integrală a datelor cu caracter personal prelucrate cu încălcarea legislaţiei în domeniul protecţiei datelor cu caracter personal,

se sancţionează cu amendă de la 30 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 60 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 150 la 300 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile, de dreptul de a desfăşura o anumită activitate pe un termen de la 3 luni la un an.

Capitolul VII

CONTRAVENŢII CE ATENTEAZĂ LA SĂNĂTATEA POPULAŢIEI, SĂNĂTATEA PERSOANEI, LA STAREA SANITAR-EPIDEMIOLOGICĂ

Articolul 75. Divulgarea informaţiei confidenţiale privind examenul medical de depistare a contaminării cu virusul imunodeficienţei umane (HIV) ce provoacă maladia SIDA

Divulgarea informaţiei confidenţiale despre examenele medicale de depistare a contaminării cu virusul imunodeficienţei umane (HIV) ce provoacă maladia SIDA de către personalul medical sau de către alte persoane care, în virtutea obligaţiilor de serviciu, deţin astfel de informaţii

se sancţionează cu amendă de la 30 la 42 de unităţi convenţionale.

Articolul 90[1]. Activităţi publice cu impact negativ asupra minorilor

(1) Difuzarea informaţiei publice cu impact negativ asupra minorilor şi/sau încălcarea legislaţiei privind protecţia minorilor de impactul negativ al informaţiei publice, altele decît cele prevăzute la alin. (2),

se sancţionează cu amendă de la 48 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 60 la 120 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 180 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile, de dreptul de a exercita o anumită activitate pe un termen de la 3 luni la un an.

(2) Difuzarea informaţiei publice şi/sau săvîrşirea unor fapte îndreptate spre propagarea prostituţiei, pedofiliei sau pornografiei

se sancţionează cu amendă de la 60 la 72 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 120 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 180 la 240 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile, de dreptul de a exercita o anumită activitate pe un termen de la 3 luni la un an.

Capitolul VIII

CONTRAVENŢII CE ATENTEAZĂ

LA DREPTURILE REALE

Articolul 92. Tăinuirea informaţiei despre fondul funciar disponibil

Tăinuirea informaţiei despre fondul funciar disponibil sau încălcarea termenelor de examinare a cererilor persoanei fizice privind atribuirea de terenuri

se sancţionează cu amendă de la 24 la 30 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere cu sau fără privarea de dreptul de a desfăşura o anumită activitate pe un termen de la 3 luni la un an.

Articolul 107. Obţinerea sau divulgarea informaţiilor care constituie secret comercial, bancar sau fiscal

(1) Obţinerea fără consimţămîntul titularului a informaţiilor care constituie secret comercial, bancar sau fiscal în scopul divulgării sau folosirii lor ilegale

se sancţionează cu amendă de la 18 la 42 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere.

(2) Divulgarea informaţiilor ce constituie secret comercial, bancar sau fiscal de către un funcţionar public sau de către o persoană căreia aceste informaţii i-au fost încredinţate sau i-au devenit cunoscute în legătură cu serviciul ei

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 150 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere.

Capitolul XIV

CONTRAVENŢII ÎN DOMENIUL COMUNICAŢIILOR ELECTRONICE, COMUNICAŢIILOR POŞTALE ŞI AL TEHNOLOGIEI INFORMAŢIEI

Articolul 246. Furnizarea neautorizată a reţelelor sau a serviciilor de comunicaţii electronice sau de tehnologie a informaţiei

(1) Furnizarea neautorizată a reţelelor sau a serviciilor de comunicaţii electronice

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 180 de unităţi convenţionale aplicată persoanei juridice.

(2) Furnizarea reţelelor sau a serviciilor de comunicaţii electronice într-o perioadă în care dreptul de furnizare a acestor reţele sau servicii a fost suspendat sau retras

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 150 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 180 la 300 de unităţi convenţionale aplicată persoanei juridice.

(3) – abrogat.

(4) – abrogat.

(5) Furnizarea neautorizată a serviciilor de tehnologie a informaţiei

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 180 de unităţi convenţionale aplicată persoanei juridice.

(6) Furnizarea serviciilor de tehnologie a informaţiei într-o perioadă în care dreptul de furnizare a acestor servicii a fost suspendat sau retras

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 150 de unităţi convenţionale apli-

cată persoanei cu funcţie de răspundere, cu amendă de la 180 la 300 de unităţi convenţionale aplicată persoanei juridice.

Articolul 247. Nerespectarea condiţiilor de autorizare general

(1) Nerespectarea condiţiilor de autorizare generală de către furnizorii de reţele sau de servicii de comunicaţii electronice sau de tehnologie a informaţiei

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 45 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

(2) Nerespectarea prescripţiei privind remedierea încălcării obligaţiilor stabilite în condiţiile de autorizare general

se sancţionează cu amendă de la 45 la 72 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 60 la 150 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 240 la 300 de unităţi convenţionale aplicată persoanei juridice cu privarea, în toate cazurile, de dreptul de a desfăşura o anumită activitate pe un termen de la 6 luni la un an.

Articolul 248. Utilizarea fără licenţă şi fără permis tehnic a canalelor, a frecvenţelor radio, a resurselor de numerotare

(1) Utilizarea fără licenţă şi fără permis tehnic a canalelor, a frecvenţelor radio

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 72 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 240 la 300 de unităţi convenţionale aplicată persoanei juridice.

(2) Utilizarea fără licenţă a resurselor de numerotare în scopul furnizării reţelelor şi/sau serviciilor de comunicaţii electronice

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 72 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 240 la 300 de unităţi convenţionale aplicată persoanei juridice.

Articolul 249. Nerespectarea condiţiilor prevăzute în licenţele de utilizare a canalelor, a frecvenţelor radio, a resurselor de numerotare

(1) Nerespectarea condiţiilor prevăzute în licenţele de utilizare a canalelor, a frecvenţelor radio, a resurselor de numerotare

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

(2) Nerespectarea prescripţiei privind remedierea încălcării obligaţiilor stabilite în condiţiile licenţei

se sancţionează cu amendă de la 42 la 72 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 60 la 120 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 108 la 210 unităţi convenţionale aplicată persoanei juridice cu privarea de dreptul de a desfăşura o anumită activitate pe un termen de la 6 luni la un an.

Articolul 249[1]. Încălcarea legislaţiei şi a reglementărilor privind accesul pe proprietăţi şi utilizarea partajată a infrastructurii asociate reţelelor publice de comunicaţii electronice

(1) Necomunicarea (netransmiterea) autorităţii de reglementare a informaţiei privind condiţiile de acces pe proprietăţi şi/sau de utilizare partajată a infrastructurii fizice stabilite conform legislaţiei şi despre oricare modificări şi/sau completări ale acestor condiţii, de asemenea netransmiterea unei copii de pe materialul cuprinzînd aceste condiţii, publicat pe pagina web oficială, dacă aceasta există, în termen de 3 zile lucrătoare de la data publicării acestuia

se sancţionează cu amendă de la 42 la 72 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei juridice.

Articolul 250. Nerespectarea reglementărilor şi a normelor tehnice din domeniul comunicaţiilor electronice, poştale şi al tehnologiei informaţiei

(1) Încălcarea normelor tehnice privind mijloacele radioelectronice, utilizate în scopuri civile, care emit unde electromagnetice

se sancţionează cu amendă de la 30 la 42 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 36 la 60 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

(2) Nerespectarea prescripţiei privind remedierea încălcării reglementărilor din domeniul comunicaţiilor electronice sau al tehnologiei informaţiei

se sancţionează cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 120 de unităţi

convenționale aplicată persoanei juridice cu privarea de dreptul de a desfăşura o anumită activitate pe un termen de la 6 luni la un an.

(2[1]) Omiterea executării prescripției cu privire la remedierea abaterilor de la reglementările în domeniul comunicațiilor poştale sau de la normele tehnice privind mijloacele radioelectronice utilizate în scopuri civile care emit unde electromagnetice

se sancționează cu amendă de la 42 la 90 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 60 la 120 de unități convenționale aplicată persoanei juridice cu privarea de dreptul de a desfăşura o anumită activitate pe un termen de la 6 luni la un an.

(3) Utilizarea sau conectarea la reţelele de comunicaţii electronice a echipamentelor de comunicaţii electronice sau poştale care nu sînt însoţite de declaraţia de conformitate emisă de producător, reprezentantul său autorizat ori importator în baza certificatului de conformitate ori a rapoartelor de încercări, sau care nu sînt marcate conform reglementărilor tehnice aplicabile

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

(4) Instalarea sau utilizarea neautorizată a echipamentelor de radiocomunicaţii de emisie în mijloacele de transport

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

(5) Crearea şi operarea neautorizată a mijloacelor de comunicaţii electronice susceptibile să cauzeze prejudicii sănătăţii oamenilor care locuiesc în zona lor de influenţă

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

(6) Încălcarea regulilor de protecţie a liniilor şi instalaţiilor de comunicaţii electronice

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale apli-

cată persoanei cu funcţie de răspundere, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

(7) Executarea lucrărilor de construcţie în zonele de protecţie a liniilor, cablurilor şi instalaţiilor de comunicaţii electronice fără autorizaţia proprietarului acestor linii, cabluri şi instalaţii

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 102 la 180 de unităţi convenţionale aplicată persoanei juridice.

(8) Instalarea sau utilizarea staţiilor de radiocomunicaţii, inclusiv a antenelor de emisie, fără coordonarea cu organul abilitat şi fără obţinerea de la acesta a autorizaţiei de utilizare

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 300 de unităţi convenţionale aplicată persoanei juridice.

(9) Plasarea pe piaţă a echipamentelor de comunicaţii electronice sau poştale care nu sînt însoţite de declaraţia de conformitate emisă de producător, reprezentantul său autorizat ori importator în baza certificatului de conformitate ori a rapoartelor de încercări, sau care nu sînt marcate conform reglementărilor tehnice aplicabile

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice.

Articolul 251. Încălcarea normelor de emisie electromagnetică şi de perturbaţii industriale admisibile pentru radiorecepţie, împiedicarea recepţionării programelor audiovizuale sau a funcţionării echipamentelor şi reţelelor de comunicaţii electronice

(1) Producerea în orice mod a perturbaţiilor prejudiciabile echipamentelor şi reţelelor de comunicaţii electronice

se sancţionează cu amendă de la 12 la 30 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 18 la 42 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 120 de unităţi convenţionale aplicată persoanei juridice.

(2) Încălcarea parametrilor tehnici de emisie autorizaţi

se sancționează cu amendă de la 6 la 30 de unități convenționale aplicată persoanei fizice, cu amendă de la 18 la 42 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 60 la 90 de unități convenționale aplicată persoanei juridice.

(3) Emisia electromagnetică intenționată, care produce perturbații prejudiciabile altor mijloace tehnice de radiocomunicații,

se sancționează cu amendă de la 30 la 42 de unități convenționale aplicată persoanei fizice, cu amendă de la 30 la 60 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 60 la 240 de unități convenționale aplicată persoanei juridice.

(4) Împiedicarea funcționării echipamentelor sau a rețelelor de comunicații electronice

se sancționează cu avertisment ori cu amendă de la 6 la 18 unități convenționale aplicată persoanei fizice, cu amendă de la 15 la 30 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 42 la 90 de unități convenționale aplicată persoanei juridice.

(5) Încălcarea normelor de emisie electromagnetică sau de perturbații industriale admisibile pentru radiorecepție, împiedicarea recepționării programelor audiovizuale

se sancționează cu amendă de la 18 la 42 de unități convenționale aplicată persoanei fizice, cu amendă de la 30 la 90 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 60 la 240 de unități convenționale aplicată persoanei juridice.

Articolul 252. Conectarea neautorizată sau admiterea conectării neautorizate la rețelele de comunicaţii electronice

Conectarea neautorizată sau admiterea conectării neautorizate a echipamentelor terminale sau a altor mijloace de comunicaţii electronice la rețelele de comunicaţii electronice, inclusiv la liniile de abonat,

se sancționează cu amendă de la 30 la 90 de unități convenţionale aplicată persoanei fizice, cu amendă de la 36 la 120 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 240 la 300 de unităţi convenţionale aplicată persoanei juridice.

Articolul 253. Refuzul neîntemeiat al furnizorului autorizat de rețele sau de servicii de a conecta la rețele sau la servicii un alt furnizor

autorizat de reţele sau de servicii

Refuzul neîntemeiat al unui furnizor autorizat de reţele sau de servicii de a conecta la reţelele sau la serviciile sale un alt furnizor autorizat de reţele sau de servicii

se sancţionează cu amendă de la 18 la 36 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 150 de unităţi convenţionale aplicată persoanei juridice.

Articolul 254. Executarea lucrărilor în domeniul comunicaţiilor electronice fără acordul proprietarului terenului sau al unui alt bun imobil ori în lipsa hotărîrii judecătoreşti privind executarea acestor lucrări

Executarea lucrărilor în domeniul comunicaţiilor electronice fără acordul proprietarului terenului sau al unui alt bun imobil ori în lipsa hotărîrii judecătoreşti privind executarea acestor lucrări

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 240 la 300 de unităţi convenţionale aplicată persoanei juridice.

Articolul 255. Deteriorarea intenţionată a liniilor, instalaţiilor, echipamentelor de comunicaţii electronice şi poştale

Deteriorarea intenţionată a liniilor, instalaţiilor, echipamentelor de comunicaţii electronice şi poştale

se sancţionează cu amendă de la 24 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 120 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 30 la 300 de unităţi convenţionale aplicată persoanei juridice.

Articolul 256. Francarea trimiterilor poştale cu mărci poştale utilizate sau neautorizate

Francarea trimiterilor poştale cu mărci poştale utilizate sau neautorizate de Ministerul Economiei şi Infrastructurii

se sancţionează cu amendă de la 2 la 4 unităţi convenţionale aplicată persoanei fizice, cu amendă de la 6 la 12 unităţi convenţionale aplicată persoanei cu

funcţie de răspundere, cu amendă de la 6 la 30 de unităţi convenţionale aplicată persoanei juridice.

Articolul 257. Confecţionarea pentru desfacere ori desfacerea cu bună ştiinţă de mărci poştale false, de clişee ale maşinilor de francare sau de sigilii poştale

Confecţionarea pentru desfacere ori desfacerea cu bună ştiinţă de mărci poştale false, de clişee ale maşinilor de francare sau de sigilii poştale

se sancţionează cu amendă de la 24 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 36 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 180 de unităţi convenţionale aplicată persoanei juridice.

Articolul 258. Predarea spre expediere a obiectelor care prezintă pericol sau a obiectelor cu caracter obscen

Predarea spre expediere prin orice tip de trimitere poştală a obiectelor care, la manipulare sau la transport, prezintă pericol pentru sănătatea oamenilor, a obiectelor cu caracter obscen fără a declara natura lor reală

se sancţionează cu amendă de la 6 la 12 unităţi convenţionale aplicată persoanei fizice, cu amendă de la 24 la 36 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere.

Articolul 259. Refuzul neîntemeiat de a furniza servicii publice în domeniul comunicaţiilor electronice şi al tehnologiei informaţiei

Refuzul neîntemeiat de a furniza servicii publice în domeniul comunicaţiilor electronice şi al tehnologiei informaţiei

se sancţionează cu amendă de la 6 la 12 unităţi convenţionale aplicată persoanei fizice, cu amendă de la 70 la 120 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 240 de unităţi convenţionale aplicată persoanei juridice.

Articolul 259[1]. Refuzul neîntemeiat de a furniza servicii publice în domeniul comunicaţiilor poştale

Refuzul neîntemeiat de a furniza servicii publice în domeniul comunicaţiilor poştale

se sancţionează cu amendă de la 18 la 36 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 42 la 90 de unităţi convenţionale aplicată per-

soanei cu funcție de răspundere, cu amendă de la 60 la 150 de unități convenționale aplicată persoanei juridice.

Articolul 260. *– abrogat*

Articolul 261. Proiectarea sau producerea fără scop de comercializare, deţinerea sau utilizarea ilegală a mijloacelor tehnice speciale pentru obţinerea ascunsă a informaţiei

(1) Proiectarea sau producerea fără scop de comercializare, deţinerea sau utilizarea ilegală a mijloacelor tehnice speciale pentru obţinerea ascunsă a informaţiei

se sancţionează cu amendă de la 18 la 30 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 60 la 120 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea de dreptul de a desfăşura o anumită activitate pe un termen de la 6 luni la un an.

(2) Utilizarea în activitatea particulară de detectiv şi de pază a mijloacelor tehnice speciale pentru obţinerea ascunsă a informaţiei

se sancţionează cu amendă de la 24 la 30 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 120 la 240 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea de dreptul de a desfăşura o anumită activitate pe un termen de la 6 luni la un an.

Articolul 262. Încălcarea regulilor de import, export, proiectare, producere şi comercializare a mijloacelor tehnice speciale pentru obţinerea ascunsă a informaţiei, nerespectarea altor condiţii de licenţiere

Încălcarea regulilor de import, export, proiectare, producere şi comercializare a mijloacelor tehnice speciale pentru obţinerea ascunsă a informaţiei, în cazul prezenţei licenţei, nerespectarea altor condiţii de licenţiere

se sancţionează cu amendă de la 18 la 30 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 48 la 90 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 120 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea de dreptul de a desfăşura o anumită activitate pe un termen de la 6 luni la un an.

Capitolul XV

CONTRAVENŢII CE AFECTEAZĂ ACTIVITATEA DE ÎNTREPRINZĂTOR, FISCALITATEA, ACTIVITATEA VAMALĂ ŞI VALORILE MOBILIARE

Articolul 279. Prezentarea de informaţii neautentice sau incomplete despre caracteristicile produselor şi ale serviciilor

Prezentarea de informaţii neautentice sau incomplete despre caracteristicile produselor şi ale serviciilor la etapa plasării pe piaţă şi/sau comercializării, trecerea sub tăcere a indicilor calitativi, a proprietăţilor produselor şi a regulilor de folosire a lor

se sancţionează cu amendă de la 6 la 42 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 120 de unităţi convenţionale aplicată persoanei juridice.

Articolul 291[6]. Neasigurarea confidenţialităţii

(1) Comunicarea de către entităţile raportoare sau de către angajaţii acestora persoanelor fizice sau juridice care efectuează tranzacţia sau activitatea ori persoanelor terţe despre transmiterea informaţiilor la Serviciul Prevenirea şi Combaterea Spălării Banilor

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei juridice.

(2) Neasigurarea de către entităţile raportoare a păstrării secretului comercial, bancar sau profesional în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului

se sancţionează cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei juridice.

(3) Neasigurarea de către angajaţii organelor cu funcţii de supraveghere a păstrării secretului comercial, bancar sau profesional în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată

persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere.

Articolul 291[7]. Neprezentarea informaţiei de către entităţile raportoare

Neprezentarea de către entităţile raportoare, la solicitarea Serviciului Prevenirea şi Combaterea Spălării Banilor, în termenele stabilite, a informaţiei disponibile privind relaţiile lor de afaceri şi natura acestor relaţii

se sancţionează cu amendă de la 60 la 90 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 90 la 180 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 180 la 300 de unităţi convenţionale aplicată persoanei juridice cu sau fără privarea, în toate cazurile, de dreptul de a desfăşura o anumită activitate pe un termen de la 3 luni la un an.

Capitolul XIX

CONTRAVENŢII CE ATENTEAZĂ LA ORDINEA PUBLICĂ ŞI LA SECURITATEA PUBLICĂ

Articolul 365[2]. Secretizarea/desecretizarea neîntemeiată a informaţiilor

(1) Secretizarea/desecretizarea informaţiilor cu încălcarea cerinţelor stabilite de legislaţia cu privire la secretul de stat

se sancţionează cu amendă de la 30 la 120 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 150 de unităţi convenţionale aplicată persoanei juridice.

(2) Refuzul neîntemeiat de a secretiza/desecretiza informaţiile atribuite la secretul de stat

se sancţionează cu amendă de la 30 la 120 de unităţi convenţionale aplicată persoanei cu funcţie de răspundere, cu amendă de la 60 la 150 de unităţi convenţionale aplicată persoanei juridice.

PARLAMENTUL

COD *Nr. 985 din 18-04-2002*

CODUL PENAL AL REPUBLICII MOLDOVA*

Publicat : 14-04-2009 în Monitorul Oficial Nr. 72-74 art. 195

MODIFICAT LP116 din 09.07.20, MO193/27.07.20, art.372; în vigoare 27.07.20

Capitolul II

INFRACŢIUNEA

Articolul 14. Noţiunea de infracţiune

(1) Infracţiunea este o faptă (acţiune sau inacţiune) prejudiciabilă, prevăzută de legea penală, săvîrşită cu vinovăţie şi pasibilă de pedeapsă penală.

(2) Nu constituie infracţiune acţiunea sau inacţiunea care, deşi, formal, conţine semnele unei fapte prevăzute de prezentul cod, dar, fiind lipsită de importanţă, nu prezintă gradul prejudiciabil al unei infracţiuni.

Capitolul V
INFRACŢIUNI CONTRA DREPTURILOR POLITICE, DE MUNCĂ ŞI ALTOR DREPTURI CONSTITUŢIONALE ALE CETĂŢENILOR

Articolul 177. Încălcarea inviolabilităţii vieţii personale

(1) Culegerea ilegală sau răspîndirea cu bună-ştiinţă a informaţiilor, ocrotite de lege, despre viaţa personală ce constituie secret personal sau familial al altei persoane fără consimţămîntul ei

se pedepseşte cu amendă în mărime de pînă la 650 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 180 la 240 de ore.

(1^1) Culegerea ilegală a informaţiilor menţionate la alin.(1), fără consimţămîntul persoanei, cu utilizarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei, se pedepseşte cu amendă în mărime de la 550 la 750 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 200 la 240 de ore.

(2) Răspîndirea informaţiilor menţionate la alin.(1):

a) într-un discurs public, prin mass-media;

b) prin folosirea intenţionată a situaţiei de serviciu

se pedepseşte cu amendă în mărime de la 550 la 850 unităţi convenţionale sau cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de 1 an, sau cu muncă neremunerată în folosul comunităţii de la 180 la 240 de ore, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 3000 unităţi convenţionale.

Articolul 178. Violarea dreptului la secretul corespondenţei

(1) Violarea dreptului la secretul scrisorilor, telegramelor, coletelor şi altor trimiteri poştale, al convorbirilor telefonice şi înştiinţărilor telegrafice, cu încălcarea legislaţiei,

se pedepseşte cu amendă în mărime de pînă la 550 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 120 la 180 de ore.

(2) Aceeaşi acţiune săvîrşită:

a) cu folosirea situaţiei de serviciu;

b) prin utilizarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei;

c) în interesul unui grup criminal organizat sau al unei organizaţii criminale

se pedepseşte cu amendă de la 550 la 750 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 100 la 240 de ore, sau cu închisoare de pînă la 3 ani, sau cu privarea de dreptul de a ocupa anumite funcţii sau de a desfăşura o anumită activitate pe un termen de pînă la 3 ani.

Articolul 180. Încălcarea intenţionată a legislaţiei privind accesul la informaţie

Încălcarea intenţionată de către o persoană cu funcţie de răspundere a procedurii legale de asigurare şi de realizare a dreptului de acces la informaţie, încălcare ce a cauzat daune în proporţii considerabile drepturilor şi intereselor ocrotite de lege ale persoanei care a solicitat informaţii referitoare la ocrotirea sănătăţii populaţiei, la securitatea publică, la protecţia mediului,

se pedepseşte cu amendă de la 500 la 650 unităţi convenţionale cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 3 ani.

Articolul 180[1]. Împiedicarea intenţionată a activităţii mass-media sau intimidarea pentru critică

(1) Împiedicarea intenţionată a activităţii mass-media sau a jurnalistului, precum și intimidarea mass-media sau a jurnalistului pentru critică

se pedepsesc cu amendă în mărime de la 500 la 650 unităţi convenţionale cu (sau fără) privarea de dreptul de a ocupa anumite funcţii publice pe un termen de pînă la 2 ani.

(2) Aceleaşi acţiuni săvîrşite cu folosirea situaţiei de serviciu

se pedepsesc cu amendă în mărime de la 650 la 850 unităţi convenţionale cu (sau fără) privarea de dreptul de a ocupa anumite funcţii publice pe un termen de pînă la 4 ani.

(3) Acţiunile prevăzute la alin. (1) și (2):

a) săvîrşite cu aplicarea violenţei sau cu ameninţarea aplicării ei;

b) săvîrşite de două sau mai multe persoane;

c) însoţite de sustragerea sau deteriorarea materialelor sau echipamentului jurnalistului în scopul împiedicării activității jurnalistice,

se pedepsesc cu amendă în mărime de la 750 la 1350 unităţi convenţionale cu (sau fără) privarea de dreptul de a ocupa anumite funcţii publice pe un termen de pînă la 5 ani.

Articolul 180[2]. Cenzura

(1) Denaturarea nejustificată a materialului jurnalistic sau interdicţia nejustificată de a răspîndi anumite informaţii, impusă de către conducerea mass-media publice,

se pedepseşte cu amendă de la 650 la 850 unităţi convenţionale cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 5 ani.

(2) Indicaţia funcţionarului public sau a persoanei care exercită funcţie de demnitate publică cu privire la activitatea editorială dată mass-media sau angajaţilor mass-media, precum și orice altă formă de împiedicare a tirajării sau răspîndirii informaţiei

se pedepsesc cu amendă de la 650 la 1350 unităţi convenţionale cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 5 ani.

Articolul 245[3]. Utilizarea abuzivă a informaţiilor privilegiate pe piaţa de capital

(1) Utilizarea de către orice persoană a informaţiilor privilegiate cu intenţia de a dobîndi sau înstrăina, pe cont propriu sau pe contul unei terţe persoane, direct ori indirect, instrumente financiare la care aceste informaţii se referă, dacă aceste acţiuni au cauzat daune în proporţii mari, se pedepseşte cu amendă în mărime de la 1350 la 2350 unităţi convenţionale sau cu închisoare de pînă la 2 ani, în ambele cazuri cu (sau fără) privarea de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

(2) Aceleaşi acţiuni:

urmate de dobîndirea sau înstrăinarea de instrumente financiare; care au cauzat daune în proporţii deosebit de mari,

se pedepsesc cu amendă în mărime de la 1350 la 3350 unităţi convenţionale sau cu închisoare de la 1 la 6 ani, în ambele cazuri cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de la 2 la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

Articolul 245[5]. Refuzul intenţionat de a dezvălui şi / sau prezenta informaţiile prevăzute de legislaţia privind piaţa financiară nebancară sau bancară

(1) Refuzul intenţionat de a dezvălui şi/sau a prezenta informaţii privind activitatea economico-financiară a societăţii pe acţiuni, deţinerile de acţiuni, rapoartele, declaraţiile, actele de constituire ori evenimentele care influenţează emitentul, informaţii a căror prezentare ori dezvăluire este obligatorie, sau prezentarea intenţionată a unor informaţii neautentice, denaturate ori false, dacă aceste acţiuni au cauzat daune în proporţii mari,

se pedepseşte cu amendă în mărime de la 2350 la 3350 unităţi convenţionale, iar persoana juridică se pedepseşte cu amendă în mărime de la 4000 la 7000 unităţi convenţionale.

(2) Aceleaşi acţiuni care au cauzat daune în proporţii deosebit de mari sau au condus la intentarea procesului de insolvabilitate,

se pedepsesc cu amendă în mărime de la 2350 la 3350 unităţi convenţionale

sau cu închisoare de la 1 la 6 ani, în ambele cazuri cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de la 2 la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

Articolul 245[10]. Obţinerea ilegală şi / sau divulgarea informaţiilor ce constituie secret comercial sau bancar

(1) Colectarea de informaţii care constituie secret comercial sau bancar prin sustragerea de informaţii, inclusiv folosirea mijloacelor tehnice speciale, extorcare sau ameninţarea cu aplicarea violenţei nepericuloase pentru viaţa sau sănătatea persoanei,

se pedepseşte cu amendă în mărime de la 1350 la 4350 unităţi convenţionale sau cu închisoare de la 1 la 6 ani, în ambele cazuri cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 3 ani.

(2) Divulgarea ilicită sau utilizarea informaţiilor ce constituie secret comercial sau bancar de către persoana căreia i-a fost încredinţată sau i-a devenit cunoscută această informaţie în virtutea atribuţiilor deţinute, fără consimţămîntul proprietarului informaţiei,

se pedepseşte cu amendă în mărime de la 1350 la 3350 unităţi convenţionale sau cu închisoare de la 1 la 3 ani, în ambele cazuri cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 5 ani.

(3) Aceleaşi acţiuni care au cauzat daune în proporţii deosebit de mari,

se pedepsesc cu amendă în mărime de la 4350 la 5350 unităţi convenţionale sau cu închisoare de la 2 la 5 ani, în ambele cazuri cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de la 2 la 5 ani.

Articolul 245[12]. Încălcarea legislaţiei privind activitatea birourilor istoriilor de credit

(1) Obţinerea, utilizarea în alte scopuri sau în alt mod decît cel prevăzut în lege şi / sau divulgarea în orice formă de către birourile istoriilor de credit, utilizatorii istoriei de credit, sursele de formare a istoriei de credit, precum şi de către persoanele cu funcţie de răspundere ale acestora a informaţiei care constituie secret comercial al biroului istoriilor de credit, al sursei de formare a istoriei de credit, al subiectului istoriei de credit sau al utilizatorului istoriei de credit,

dacă aceste acţiuni au cauzat daune în proporţii mari,

se pedepseşte cu amendă în mărime de la 850 la 2350 unităţi convenţionale cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 2000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Neprezentarea intenționată a informației în volumul stabilit de lege sau prezentarea eronată a acesteia în mod intenționat la biroul istoriilor de credit de către sursele de formare a istoriilor de credit, precum şi de către persoanele cu funcţie de răspundere ale acestora, dacă aceste acţiuni au cauzat daune în proporţii mari,

se pedepseşte cu amendă în mărime de la 850 la 2350 de unităţi convenţionale cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 2000 la 4000 de unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(3) Furnizarea și/sau folosirea, și/sau administrarea ilegală a informațiilor ce caracterizează respectarea de către debitori a obligațiilor asumate prin contractele de credit și/sau contractele de împrumut de către persoanele juridice ce nu dețin licențe pentru activitatea biroului istoriilor de credit, precum şi de către persoanele cu funcție de răspundere ale acestora, dacă aceste acțiuni au cauzat daune în proporții mari,

se pedepsesc cu amendă în mărime de la 850 la 2350 de unități convenționale cu (sau fără) privarea de dreptul de a ocupa anumite funcții sau de a exercita o anumită activitate pe un termen de pînă la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 2000 la 4000 de unități convenționale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

(4) Acțiunile prevăzute la alin. (1), (2) sau (3) care au cauzat daune în proporții deosebit de mari

se pedepsesc cu amendă în mărime de la 1350 la 3350 de unități convenționale sau cu închisoare de pînă la 3 ani, în ambele cazuri cu (sau fără) privarea de dreptul de a ocupa anumite funcții sau de a exercita o anumită activitate pe un termen de la 2 la 5 ani, iar persoana juridică se pedepsește cu amendă în mărime de la 4000 la 7000 de unități convenționale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

Capitolul XI
INFRACŢIUNI INFORMATICE ŞI INFRACŢIUNI ÎN DOMENIUL TELECOMUNICAŢIILOR

Articolul 259. Accesul ilegal la informaţia computerizată

(1) Accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică, al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic, dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice şi dacă a cauzat daune în proporţii mari,

se pedepseşte cu amendă în mărime de la 550 la 850 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare de pînă la 2 ani, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 4000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Aceeaşi acţiune săvîrşită:

a) - *exclusă*

b) de două sau mai multe persoane;

c) cu violarea sistemelor de protecţie;

d) cu conectarea la canalele de telecomunicaţii;

e) cu folosirea unor mijloace tehnice special

f) cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvîrşirii uneia dintre infracţiunile prevăzute la alin.(1), la art.260^1–260^3, 260^5 şi 260^6;

g) în privinţa informaţiei protejată de lege;

h) în proporţii deosebit de mari.

se pedepseşte cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 180 la 240 de ore, sau cu închisoare de pînă la 3 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a

exercita o anumită activitate sau cu lichidarea persoanei juridice.

Articolul 260. Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program

Producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal, a mijloacelor tehnice sau produselor program, concepute sau adaptate, în scopul săvîrşirii uneia dintre infracţiunile prevăzute la art.237, 259, 260^{1}–260^{3}, 260^{5} şi 260^{6};

se pedepseşte cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

Articolul 260^{1}. Interceptarea ilegală a unei transmisii de date informatice

Interceptarea ilegală a unei transmisii de date informatice (inclusiv a unei emisii electronice) care nu sînt publice şi care sînt destinate unui sistem informatic, provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatics

se pedepseşte cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

Articolul 260^{2}. Alterarea integrităţii datelor informatice ţinute într-un sistem informatics

Modificarea, ştergerea sau deteriorarea intenţionată a datelor informatice ţinute într-un sistem informatic ori restricţionarea ilegală a accesului la aceste date, transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobîndirea, comercializarea sau punerea la dispoziţie, sub orice formă, a datelor informatice cu acces limitat, dacă aceste acţiuni au cauzat daune în proporţii mari,

se pedepsesc cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare de la 2 la 5 ani.

Articolul 260^{3}. Perturbarea funcţionării sistemului informatics

(1) Perturbarea funcţionării unui sistem informatic prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la aceste date, dacă aceste acţiuni au cauzat daune în proporţii mari,

se pedepseşte cu amendă în mărime de la 1050 la 1350 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

(2) Aceeaşi acţiune:

a) săvîrşită din interes material;

b) săvîrşită de două sau mai multe persoane;

c) săvîrşită de un grup criminal organizat sau de o organizaţie criminală;

d) care a cauzat daune în proporţii deosebit de mari

se pedepseşte cu amendă în mărime de la 1050 la 1350 unităţi convenţionale sau cu închisoare de la 3 la 7 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale sau cu lichidarea întreprinderii.

Articolul 260^4. Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similar

(1) Producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal, a unei parole, a unui cod de acces sau a unor date similare care permit accesul total sau parţial la un sistem informatic în scopul săvîrşirii uneia dintre infracţiunile prevăzute la art.237, 259, 260^1–260^3, 260^5 şi 260^6, dacă aceste acţiuni au cauzat daune în proporţii mari,se pedepsesc cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 4000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Aceleaşi acţiuni:

a) săvîrşite din interes material;

b) săvîrşite de două sau mai multe persoane;

c) săvîrşite de un grup criminal organizat sau de o organizaţie criminală;

d) care au cauzat daune în proporţii deosebit de mari

se pedepsesc cu amendă în mărime de la 1350 la 1850 unităţi convenţionale sau cu închisoare de la 3 la 7 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii.

Articolul 260[5]. Falsul informatics

Introducerea, modificarea sau ştergerea ilegală a datelor informatice ori restricţionarea ilegală a accesului la aceste date, rezultînd date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice

se pedepsesc cu amendă în mărime de la 1350 la 1850 unităţi convenţionale sau cu închisoare de la 2 la 5 ani.

Articolul 260[6] . Frauda informatică

(1) Introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă aceste acţiuni au cauzat daune în proporţii mari,

se pedepsesc cu amendă în mărime de la 1350 la 1850 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare de la 2 la 5 ani.

(2) Aceleaşi acţiuni:

a) săvîrşite de un grup criminal organizat sau de o organizaţie criminală;

b) care au cauzat daune în proporţii deosebit de mari

se pedepsesc cu închisoare de la 4 la 9 ani.

Articolul 261. Încălcarea regulilor de securitate a sistemului informatics

Încălcarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic, prevăzute în conformitate cu statutul informaţiei sau gradul ei de protecţie, dacă această acţiune a contribuit la însuşirea, denaturarea sau la distrugerea informaţiei ori a provocat alte urmări grave,

se pedepseşte cu amendă în mărime de pînă la 750 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 200 la 240 de ore, sau cu închisoare de pînă la 2 ani, în toate cazurile cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de la 2 la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 2000 la 4000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

Articolul 261[1]. Accesul neautorizat la reţelele şi serviciile de telecomunicaţii

(1) Accesul neautorizat la reţelele şi/sau serviciile de telecomunicaţii cu utilizarea reţelelor şi/sau serviciilor de telecomunicaţii ale altor operatori, dacă acesta a cauzat daune în proporţii mari,

se pedepseşte cu amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare de pînă la 1 an, iar persoana juridică se pedepseşte cu amendă în mărime de la 2000 la 4000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Aceeaşi acţiune:

a) - *exclusă*

b) săvîrşită de două sau mai multe persoane;

c) săvîrşită cu violarea sistemelor de protecţie;

d) săvîrşită cu folosirea mijloacelor tehnice speciale;

e) care a cauzat daune în proporţii deosebit de mari

se pedepseşte cu amendă în mărime de la 1350 la 3350 unităţi convenţionale sau cu închisoare de pînă la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

Capitolul XIV
INFRACŢIUNI CONTRA JUSTIŢIEI

Articolul 316. Divulgarea datelor privind măsurile de asigurare a securităţii aplicate faţă de judecător, executorul judecătoresc, participantul la procesul penal sau angajatul organului abilitat cu protecţia martorilor

(1) Divulgarea datelor privind măsurile de asigurare a securităţii aplicate faţă de judecător, executorul judecătoresc, participantul la procesul penal sau angajatul organului abilitat cu protecţia martorilor, precum şi faţă de rudele apropiate ale acestora,

se pedepseşte cu amendă în mărime de la 550 la 750 de unităţi convenţionale sau cu închisoare de pînă la 2 ani.

(2) Aceeaşi faptă:

a) săvîrşită de către o persoană căreia aceste date i-au fost încredinţate în virtutea atribuţiilor de serviciu;

b) soldată cu urmări grave

se pedepsește cu închisoare de la 3 la 5 ani cu privarea de dreptul de a ocupa anumite funcții sau de a exercita o anumită activitate pe un termen de pînă la 5 ani.

Capitolul XV
INFRACŢIUNI CONTRA BUNEI DESFĂŞURĂRI A ACTIVITĂŢII ÎN SFERA PUBLICĂ

Articolul 330[1]. Încălcarea regimului de confidenţialitate a informaţiilor din declaraţiile de avere și interese personale

(3) Divulgarea sau publicarea intenţionată a informaţiilor din declaraţiile de avere și interese personale de către persoanele cărora aceste informaţii le-au devenit cunoscute în procesul îndeplinirii atribuţiilor de serviciu sau al exercitării controlului

se pedepseşte cu amendă în mărime de la 500 la 650 unităţi convenţionale, cu (sau fără) privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de la 1 la 5 ani.

Capitolul XVII
INFRACŢIUNI CONTRA AUTORITĂŢILOR PUBLICE ŞI A SECURITĂŢII DE STAT

Articolul 337. Trădarea de Patrie

(1) Trădarea de Patrie, adică fapta săvîrşită intenţionat de un cetăţean al Republicii Moldova în dauna suveranităţii, inviolabilităţii teritoriale sau a securităţii de stat şi a capacităţii de apărare a Republicii Moldova, prin trecerea de partea duşmanului, spionaj, divulgare a secretului de stat unui stat străin, unei organizaţii străine sau reprezentanţilor lor, precum şi acordarea de ajutor unui stat străin la înfăptuirea activităţii duşmănoase împotriva Republicii Moldova,

se pedepsesc cu închisoare de la 12 la 20 de ani.

(2) Este liberat de răspundere penală cetăţeanul Republicii Moldova, racolat de serviciul de spionaj străin pentru înfăptuirea unei activităţi duşmănoase împotriva Republicii Moldova, dacă el nu a săvîrşit nici un fel de acţiuni pentru realizarea însărcinării criminale primite şi a declarat de bună voie autorităţilor despre legătura sa cu serviciul de spionaj străin.

Articolul 338. Spionajul

Transmiterea, precum şi sustragerea sau culegerea de informaţii ce constitu-

ie secret de stat în scopul transmiterii lor unui stat străin, unei organizaţii străine sau agenturii lor, precum şi transmiterea sau culegerea, din însărcinarea serviciului de spionaj străin, a altor informaţii pentru a fi folosite în dauna intereselor Republicii Moldova, dacă spionajul este săvîrşit de un cetăţean străin sau de un apatrid,

se pedepseşte cu închisoare de la 12 la 20 de ani.

Articolul 344. Divulgarea secretului de stat

(1) Divulgarea informaţiilor ce constituie secret de stat de către o persoană căreia aceste informaţii i-au fost încredinţate sau i-au devenit cunoscute în legătură cu serviciul sau munca sa, dacă nu constituie trădare de Patrie sau spionaj,

se pedepseşte cu amendă în mărime de la 550 la 950 unităţi convenţionale sau cu închisoare de pînă la 4 ani, în ambele cazuri cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 5 ani.

(2) Aceeaşi acţiune soldată cu urmări grave

se pedepseşte cu închisoare de la 3 la 7 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de la 2 la 5 ani.

Articolul 345. Pierderea documentelor ce conţin secrete de stat

Pierderea documentelor ce conţin secrete de stat, precum şi a obiectelor datele despre care constituie secret de stat, de către o persoană căreia aceste documente sau obiecte i-au fost încredinţate, dacă pierderea a fost un rezultat al încălcării regulilor stabilite de păstrare a documentelor sau obiectelor menţionate şi a cauzat urmări grave,

se pedepseşte cu amendă în mărime de la 500 la 750 unităţi convenţionale sau cu închisoare de pînă la 3 ani, în ambele cazuri cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de pînă la 5 ani.

BIBLIOGRAFIE

ACTE NORMATIVE

ACTE NORMATIVE INTERNAȚIONALE

1. Declarația universală a drepturilor omului Adoptat prin Rezoluția Adunării Generale 217 A (III) a Adunării Generale a ONU la 10 decembrie anul 1948
2. Organizația Internațională pentru Standardizare, ISO (Organizația Internațională pentru Standardizare, ISO) Comisia Electrotehnică Internațională Standardul internațional ISO / IEC 10746-2: 1996
3. Organizația Internațională pentru Standardizare, ISO (Organizația Internațională pentru Standardizare, ISO) Comisia Electrotehnică Internațională Standardul internațional ISO / IEC 2382: 2015

ACTE NORMATIVE NAȚIONALE

1. CONSTITUȚIA Republicii Moldova din 29.07.1994 din 29.07.1994 Publicată: 12.08.1994 în Monitorul Oficial Nr. 1 Data intrării în vigoare: 27.08.1994
2. COD Nr. 218 din 24-10-2008 CODUL CONTRAVENȚIONAL AL REPUBLICII MOLDOVA*

   Publicat : 17-03-2017 în Monitorul Oficial Nr. 78-84 art. 100

   Modificat LP116 din 09.07.20, MO193/27.07.20, art.372; în vigoare 27.07.20
3. COD Nr. 985 din 18-04-2002 CODUL PENAL AL REPUBLICII MOLDOVA*

   Publicat : 14-04-2009 în Monitorul Oficial Nr. 72-74 art. 195

   Modificat LP116 din 09.07.20, MO193/27.07.20, art.372; în vigoare 27.07.20
4. COD Nr. 1107 din 06-06-2002 CODUL CIVIL AL REPUBLICII MOLDOVA

   Publicat : 22-06-2002 în Monitorul Oficial Nr. 82-86 art. 661 *Republicat în Monitorul Oficial nr.66-75 din 01.03.2019 art.132

5. COD Nr. 122 din 14-03-2003CODUL DE PROCEDURĂ PENALĂ AL REPUBLICII MOLDOVA

   Publicat : 05-11-2013 în Monitorul Oficial Nr. 248-251 art. 699

   Modificat LP99 din 11.06.20, MO161-164/03.07.20 art.313; în vigoare 03.10.20

6. COD Nr. 259 din 15.07.2004 cu privire la ştiinţă şi inovare al Republicii Moldova Publicat : 30.07.2004 în Monitorul Oficial Nr. 125-129

7. LEGEA Nr. 982 din 11.05.2000 privind accesul la informaţie Publicat : 28.07.2000 în Monitorul Oficial Nr. 88-90

8. LEGEA Nr. 216 din 29.05.2003 cu privire la Sistemul informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni Publicat : 08.08.2003 în Monitorul Oficial Nr. 170-172

9. LEGEA Nr. 467 din 21.11.2003 cu privire la informatizare şi la resursele informaţionale de stat Publicat : 01.01.2004 în Monitorul Oficial Nr. 6-12

10. LEGEA **Nr. 59 din 29-03-2012** privind activitatea specială de investigaţii

    Publicat : 08-06-2012 în Monitorul Oficial Nr. 113-118 art. 373

    Versiune în vigoare din 12.01.19 *în baza modificărilor prin* LP245 din 15.11.18 MO 462-466 din 12.12.18 art. 774

11. LEGEA Nr. 269 din 12-12-2008 privind aplicarea testării la detectorul comportamentului simulat (poligraf)

    Publicat : 20-03-2009 în Monitorul Oficial Nr. 57-58 art. 161

    Versiune în vigoare din 15.06.18 în baza modificărilor prin LP79 din 24.06.18, MO195-209/15.06.18 art.338

12. LEGEA Nr. 216 din 29-05-2003cu privire la Sistemul informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni

    Publicat : 08-08-2003 în Monitorul Oficial Nr. 170-172 art. 695

    Versiune în vigoare din data 12.01.19 în baza modificărilor prin LP245 din15.11.18 *MO* 462-466 din12.12.18 art. 774

13. LEGEA Nr. 133din 08-07-2011privind protecţia datelor cu caracter

personal Modificat LP52 din 12.03.20, MO84/14.03.20 art.88; în vigoare 14.03.20 Publicat : 24-12-2010 în Monitorul Oficial Nr. 254-256 art. 1282

14. LEGEA **Nr. 1260 din 19-07-2002**cu privire la avocatură

    Publicat : 12-09-2002 în Monitorul Oficial Nr. 126-127 art. 1001

    Modificat LP146 din 16.07.20, MO194-197/31.07.20 art.394; în vigoare 31.07.20

15. LEGEA **Nr. 69 din 14-04-2016** cu privire la organizarea activităţii notarilor

    Publicat : 26-08-2016 în Monitorul Oficial Nr. 277-287 art. 588

    Modificat LP246 din 15.11.18, MO30-37/01.02.19 art.89

16. LEGEA **Nr. 246 din 15-11-2018** privind procedura notarială

    Publicat : 01-02-2019 în Monitorul Oficial Nr. 30-37 art. 89

17. LEGEA **Nr. 271 din 15-12-2017**privind auditul situaţiilor financiare

    Publicat : 12-01-2018 în Monitorul Oficial Nr. 7-17 art. 48

    Versiune in vigoare din 01.01.19 in baza modificărilor prin LP234 din 08.11.18, MO448-460/07.12.18 art.733;

18. L E G EA nr. 202 din 06.10.2017 privind activitatea băncilor

    Monitorul Oficial al R. Moldova nr. 434-439 art. 727 din 15.12.2017

19. LEGEA **Nr. 113 din 17-06-2010** privind executorii judecătoreşti*

    Publicat : 06-01-2017 în Monitorul Oficial Nr. 2-8 art. 01

    Versiune în vigoare din 30.12.18 în baza modificărilor prin LP238 din 08.11.18, *MO*441-447 din 30.11.18 art.709

20. LEGEA **Nr. 283 din 04-07-2003** privind activitatea particulară de detectiv şi de pază

    Publicat : 19-09-2003 în Monitorul Oficial Nr. 200-203 art. 769

    Versiune in vigoare din 12.01.19 in baza modificărilor prin LP245 din 15.11.18 *MO* 462-466 din 12.12.18 art. 774

21. LEGEA **Nr. 264din 27-10-2005** cu privire la exercitarea profesiunii de medic

    Publicat : 23-12-2005 în Monitorul Oficial Nr. 172-175 art. 839

Versiune în vigoare din 30.12.18 în baza modificărilor prin LP238 din 08.11.18 *MO*441-447 din 30.11.18 art. 709

22. LEGEA **Nr. 243 din 26-10-1994** Presei

    Publicat : 12-01-1995 în Monitorul Oficial Nr. 2 art. 12

23. LEGEA **Nr. 125 din 11-05-2007** Lege privind libertatea de conştiinţă, de gîndire şi de religie

    Publicat : 17-08-2007 în Monitorul Oficial Nr. 127-130 art. 546

24. LEGEA **Nr. 30 din 07-03-2013** cu privire la protecţia copiilor împotriva impactului negativ al informaţiei

    Publicat : 05-04-2013 în Monitorul Oficial Nr. 69-74 art. 221

25. LEGEA **Nr. 20 din 03-02-2009** privind prevenirea şi combaterea criminalităţii informatice

    Publicat : 26-01-2010 în Monitorul Oficial Nr. 11-12 art. 17

    Versiune în vigoare din 15.06.18 în baza modificărilor prin LP79 din 24.05.18, MO195-209/15.06.18 art.338

26. LEGEA **Nr. 91din 27-06-2014** privind semnătura electronică şi documentul electronic

    Publicat : 04-07-2014 în Monitorul Oficial Nr. 174-177 art. 397

    Modificat LP317 din 30.11.18, MO1-5/04.01.19 art.40; în vigoare 04.02.19

27. HOTĂRÎRE Nr. 1123 din 14-12-2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal

28. HOTĂRÎRE Nr. 449 din 16-06-2011cu privire la aprobarea Nomenclatorului persoanelor cu funcţii de răspundere cu împuterniciri de atribuire a informaţiilor la secret de stat

    Publicat : 24-06-2011 în Monitorul Oficial Nr. 103-106 art. 513

29. HOTĂRÎRE Nr. 411 din 25-05-2010 privind aprobarea Nomenclatorului informaţiilor atribuite la secret de stat

    Publicat : 28-05-2010 în Monitorul Oficial Nr. 83-84 art. 483

    Versiune în vigoare din 16.11.18 în baza modificărilor prin HG1106

din 14.11.18, MO424-429/16.11.18 art.1175

30. HOTĂRÎRE Nr. 1176 din 22-12-2010 pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice

    Publicat : 26-08-2011 în Monitorul Oficial Nr. 139-145 art. 686

    Versiune în vigoare din 31.10.14 în baza modificărilor prin HG886 din 22.10.14, MO325-332/31.10.14 art.954

31. REGULAMENTUL privind licențierea activității de prestare a serviciilor în domeniul importului, exportului, proiectării, producerii şi comercializării mijloacelor tehnice speciale destinate pentru obținerea ascunsă a informaţiei

32. REGULAMENTUL privind licențierea activității de prestare a serviciilor în domeniul protecției criptografice a informației

33. REGULAMENTUL privind licențierea activității de prestare a serviciilor în domeniul protecției tehnice a informației

34. REGULAMENT cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice

MONOGRAFII ŞI PUBLICAȚII PERIODICE

1. Рассолов И. М. Чубукова С. Г. «Информационное право» Рабочая программа Москва. Издательский центр Университета имени О.Е. Кутафина (МГЮА) 2013 104 с.

2. Савельев Д.А. «Информационное право и информационное государство» Учебное пособие. – СПб: НИУ ИТМО, 2012. – 71 с

3. Копылов В.А. «Информационное право.» 2-е изд., перераб. и доп. – М.: Юристъ, 2002. – 512 с.

4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. «Технические средства и методы защиты информации» М.: ООО «Издательство Машиностроение», 2009 – 508 с.

5. Завгородний В.И. «Комплексная защита информации в компьютерных системах» Учебное пособие. - М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - 264 с: ил.

6. Secrieru, V. Cuşnir, S. Arhiliuc «Managementul securităţii informaţiei electronice (Curs de lecţii)» ; Universitatea de Stat de Educaţie Fizică şi Sport. - Chişinău : Editura USEFS, 2010.

7. VASIU, L. VASIU, Informatică juridică şi drept informatic 2005, Ed. Albastră, Cluj-Napoca, 2005.
8. Andronatii, V. Balmuş Cu privire la genurile şi caracteristicile informaţiei //Legea şi viaţa 11/21, 2005
9. Gh. Alecu Particularităţi ale investigaţiei penale şi criminalistice a unor infracţiuni din domeniul informatic //Avocatul poporului 8/2, 2005
10. Gh. Semenov, N. Carpov Clasificarea criminalistică a infracţiunilor în domeniul informaticii în sistemul legării celulare //Legea şi viaţa 11/25, 2005
11. Брединский «Носители информации и утечка данных: анализ международного опыта» Conferinţa internationala «Securitatea informationala 2013» Chişinau ASEM 2013
12. Bredinschi «Digital document protection system» Conferinţa internaionala «Information technologies and security 2012» Chişinau ULIM 2013
13. А. Брединский «Особенности защиты цифровых документов» Conferinţa internationala «Securitatea informationala 2012» Chişinau ASEM 2012