MINISTERUL MEDIULUI AL REPUBLICII MOLDOVA
INSPECTORATUL PENTRU PROTECȚIA MEDIULUI

MD 2028, mun. Chișinău, șos. Hîncești, 53, tel. 022-22-69-41, tel/fax 022-22-69-15,
E-mail: mediu@ipm.gov.md, WEB: www.ipm.gov.md

ORDIN

mun. Chișinău

"01" februarie 2023 Nr. 14

Cu privire la asigurarea confidențialității prelucrării datelor cu caracter personal operate de Inspectoratul pentru Protecția Mediului și subdiviziunile teritoriale ale IPM

În scopul asigurării confidențialității și securității datelor cu caracter personal ale angajaților Inspectoratului pentru Protecția Mediului, persoanelor fizice în cadrul proceselor contravenționale/civile/penale/administrative, acțiunilor de inspectare intentate în privința acestora, precum și în procesul evidenței și circulației corespondenței, conform prevederilor Legii nr.133/2011 privind protecția datelor cu caracter personal, ale Hotărîrii Guvernului nr.1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, inclusiv conform Instrucțiunii cu privire la asigurarea securității datelor cu caracter personal din cadrul Sistemului Informațional Automatizat „Registrul funcțiilor publice și al funcționarilor publici" a Cancelariei de Stat a Guvernului, precum și în scopul executării prevederilor art.13 "Evidența funcțiilor publice și ale funcționarilor publici" al Legii nr.158 –XVI din 04.07.2008 cu privire la funcția publică și statutul funcționarului public, ale Legii nr.133/2016 privind declararea averii și a intereselor personale, ale Hotărîrii Guvernului nr.673/2017 pentru implementarea legii menționate, ale anexei nr.11 la Hotărîrea Guvernului nr.201/2009, prin care este aprobată Instrucțiunea cu privire la gestionarea dosarului personal al funcționarului public, precum și în conformitate cu pct.18 subpct. 12) și 13) al Regulamentului privind organizarea și funcționarea Inspectoratului pentru Protecția Mediului, aprobat prin Hotărîrea Guvernului nr.548/2018,

ORDON:

1. Se aprobă actele administrativ – normative ale Inspectoratului, după cum urmează:

1.1. Politica de Securitate privind protecția datelor cu caracter personal prelucrate și stocate în cadrul Inspectoratului pentru Protecția Mediului;

1.2. Regulamentul privind prelucrarea datelor cu caracter personal ale angajaților Inspectoratului pentru Protecția Mediului și altor persoane fizice în

procesul de administrare a resurselor umane în cadrul Inspectoratului pentru Protecţia Mediului;

1.3. Regulamentul privind prelucrarea datelor cu caracter personal în sistemul de evidenţă contabilă a Inspectoratului pentru Protecţia Mediului;

1.4. Regulamentul privind protecţia datelor cu caracter personal în procesul evidenţei şi circulaţiei corespondenţei, atât la nivelul aparatului central al Inspectoratului pentru Protecţia Mediului, cât şi a subdiviziunilor teritoriale a acestuia.

2. Se abrogă, în totalitate, din data emiterii prezentului Ordin, Ordinul IPM nr.19 din 11.03.2021 *„Cu privire la asigurarea securităţii datelor cu caracter personal operate de Inspectoratul pentru Protecţia Mediului"*.

3. Responsabil de controlul executării prevederilor Politicii de Securitate privind protecţia datelor cu caracter personal prelucrate şi stocate în cadrul Inspectoratului pentru Protecţia Mediului şi a Regulamentelor menţionate la pct.1.1. – 1.4. se desemnează Serviciul audit intern şi securitate internă.

4. Responsabili pentru respectarea şi executarea prevederilor Politicii de Securitate privind protecţia datelor cu caracter personal prelucrate şi stocate în cadrul Inspectoratului pentru Protecţia Mediului şi a Regulamentelor menţionate la pct.1.1. – 1.4. se desemnează conducătorii Direcţiilor/Secţiilor/Serviciilor din cadrul Inspectoratului şi şefii subdiviziunilor teritoriale ale IPM în limita competenţelor atribuite.

5. Angajaţii Inspectoratului pentru Protecţia Mediului şi a subdiviziunilor teritoriale ale IPM vor prezenta Secţiei resurse umane Acordul stabilit în anexa nr.1 la Regulamentul specificat la pct.1.2. al prezentului Ordin, precum şi Angajamentul din anexa nr.1 al Ordinului în cauză, iar dna Svetlana Şebolenco, şef Secţie, va asigura plasarea acestora în dosarele personale ale funcţionarilor publici.

6. Serviciul sinteze informaţionale şi relaţii cu publicul va asigura plasarea Politicii de Securitate privind protecţia datelor cu caracter personal prelucrate şi stocate în cadrul Inspectoratului pentru Protecţia Mediului pe pagina web a Inspectoratului.

7. Prezentul Ordin se aduce la cunoştinţă angajaţilor Inspectoratului pentru Protecţia Mediului şi subdiviziunilor teritoriale.

8. Neexecutarea corespunzătoare a prevederilor prezentului Ordin constituie abatere disciplinară şi atrage după sine răspundere disciplinară.

9. Executarea prezentului Ordin se pune în sarcina persoanelor sus menţionate, iar controlul asupra executării acestuia mi-l asum.

Şef Inspectorat **Ion BULMAGA**

Anexa nr.1
la Ordinul Şefului IPM
nr. 14 din „01" 02 2023

ANGAJAMENT

privind păstrarea confidenţialităţii datelor cu caracter personal ale persoanelor fizice în cadrul proceselor contravenţionale/civile/penale/administrative, acţiunilor de inspectare intentate în privinţa acestora, precum şi în procesul evidenţei şi circulaţiei corespondenţei, atât la nivelul aparatului central al Inspectoratului pentru Protecţia Mediului, cât şi a subdiviziunilor teritoriale a acestuia

Subsemnatul/a _____, angajat/angajată în cadrul Inspectoratului pentru Protecţia Mediului (Inspecţiei pentru Protecţia Mediului), **în funcţia de** _____,

mă oblig, în conformitate cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal şi ale Hotărârii Guvernului nr.1123/2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal", să păstrez confidenţialitatea datelor cu caracter personal ale persoanelor fizice în cadrul proceselor contravenţionale intentate în privinţa acestora, precum şi în procesul evidenţei şi circulaţiei corespondenţei, şi ale angajaţilor IPM, să respect măsurile tehnice şi organizatorice, necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate.

Data _____ Semnătura _____

Aprobat
prin Ordinul Şefului IPM
nr. 14 din 01. 02. 2023

Politica de Securitate privind protecţia datelor cu caracter personal prelucrate şi stocate în cadrul Inspectoratului pentru Protecţia Mediului

Cuprins

I. Introducere

1.1. Inspectoratul pentru Protecţia Mediului (în continuare – *IPM, Inspectorat*) autoritate administrativă în subordinea Ministerului Mediului (în continuare – *autoritatea centrală de specialitate*), împuternicit să efectueze supravegherea şi controlul de stat în domeniul protecţiei mediului şi utilizării resurselor naturale, creat în baza Hotărîrii Guvernului nr.548/2018 cu privire la organizarea şi funcţionarea Inspectoratului pentru Protecţia Mediului.

1.2. Inspectoratul are sediul înregistrat în mun. Chişinău, str. Şos. Hîncești, 53, MD-2028.

1.3. La prelucrarea datelor cu caracter personal în cadrul entităţii sunt aplicate principiile prevăzute de actele normative:

1) Constituţia Republicii Moldova;

2) Legea privind protecţia datelor cu caracter personal nr.133/2011;

3) Legea privind accesul la informaţie nr.982/2000;

4) Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123/2010 (în continuare - Cerinţe);

5) Regulamentul Registrului de evidenta al operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr.296/2012;

6) alte acte normative de profil.

II. Noţiuni generale

2.1. În prezenta Politică de Securitate, sunt definite/utilizate următoarele noţiuni:

1) *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;

2) *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 constrângere sau sancţiunile contravenţionale;

3) *operator* - persoană fizică sau persoană 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;

4) *persoana împuternicită de către operator* - persoană fizică sau persoană 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;

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

6) *control de securitate* - acţiuni întreprinse de către operator în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute;

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

8) *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;

9) *politica de securitate a datelor cu caracter personal* - document, elaborat de către operatorul de date - Inspectorat, care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinându-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sunt expuse acestea;

10) *perimetru de securitate* - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace
de control fizic şi/sau tehnic al accesului, la caz, perimetrul de securitate a Inspectoratului reprezintă perimetru oficiilor în care se prelucrează/stochează date cu caracter personal;

11) *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;

12) *protecţia informaţiei contra acţiunilor neintenţionate* - ansamblu de masuri 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;

13) *purtător de date cu caracter personal*- suport magnetic, optic, laser, de hârtie 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;

14) *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;

15) *sesiune de lucru* - perioada care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei

informaţionale şi până la momentul opririi acestora;

16) *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;

17) *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;

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

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

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

21) *terţ* – persoană fizică sau persoană juridică de drept public ori de drept privat, alta decât subiectul datelor cu caracter personal, decât operatorul ori persoana împuternicită de către operator şi decât persoana care sub autoritatea directă a operatorului sau a persoanei împuternicite este autorizată să prelucreze date cu caracter personal;

22) *destinatar* – orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, căreia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu terţ. Nu sunt 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;

23) *consimţământul subiectului de date cu caracter personal* – manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate;

24) *depersonalizarea datelor* – modificarea datelor cu caracter personal astfel încât 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;

25) *creare de profiluri* – formă de prelucrare automată a datelor cu caracter personal, care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte referitoare la o persoană fizică, în special pentru a analiza sau a stabili aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele,

interesele, fiabilitatea, comportamentul, locul în care se află persoana respectivă şi deplasările acesteia.

III. Obiectivele Politicii de Securitate

3.1. Obiectivele principale ale Politicii de Securitate sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de Inspectorat, atât în cadrul prelucrării manuale, cât şi sistemelor şi proceselor de tehnologie informaţională. Securitatea reprezintă o componentă esenţiala a derulării optime a proceselor bazate pe TI în cadrul Inspectoratului. Baza unei securităţi TI adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datelor cu caracter personal, sistemelor şi proceselor TI împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv nemateriale, sau care pot duce la încălcări ale legislaţiei. Având în vedere că siguranţa TI nu poate fi garantata exclusiv cu ajutorul unor sisteme tehnice, prezenta Politica vizează, de asemenea, aspecte de ordin organizatoric-juridic şi de altă natură.

3.2. Inspectoratul va proteja datele cu caracter personal ale angajaţilor săi, a candidaţilor la funcţiile vacante, a vizitatorilor precum şi ale altor persoane ale căror date cu caracter personal vor fi prelucrate de către Inspectorat.

3.3. Reglementările prezentei Politici de Securitate reprezintă un standard minim pentru Inspectorat, inclusiv pentru toţi angajaţii acestuia. Pornind de la această reglementare, toţi salariaţii urmează să respecte strict prevederile Politicii de Securitate şi regulile interne ale Inspectoratului privind protecţia datelor cu caracter personal.

IV. Dispoziţii privind ierarhia şi responsabilitatea persoanei responsabile de Politica de Securitate

4.1. Politica de Securitate, în mod obligatoriu va fi adusa la cunoştinţă, sub semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

4.2. Persoana responsabilă de implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal este numita prin Ordinul Şefului Inspectoratului şi va avea acces liber la informaţia necesara pentru îndeplinirea funcţiilor sale în măsură în care aceasta nu operează în afara cadrului acestei politici şi se subordonează nemijlocit Şefului Inspectoratului sau persoanei care îndeplineşte interimatul funcţiei.

V. Descrierea procedurilor (organizatorice şi tehnice) de prelucrare şi de securitate

5.1. *Mijloace supuse principiilor de protecţie a datelor cu caracter personal:*

Sunt supuse protecţiei prin mijloace/procedee specifice, toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin date

cu caracter personal, păstrate pe:

1) suporturi magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;

2) 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.

Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin:

1) preîntâmpinarea conexiunilor neautorizate la reţelele comunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;

2) excluderea accesului neautorizat la datele cu caracter personal prelucrate;

3) preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

4) preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

5) preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătura, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea canalelor virtuale protejate (VPN);

6) preîntâmpinarea 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 anti-virus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodica a copiilor de siguranţă;

7) preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent;

8) stabilirea exacta a ordinii de acces la informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenta instituite atât pentru utilizatorii interni cât şi pentru cei externi.

5.2. *Măsurile generale de administrare a securităţii informaţionale:*

1) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.

2) Computerele, terminalele de acces şi imprimantele sunt deconectate la terminarea sesiunilor de lucru.

3) Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.

4) Este asigurată securitatea şi accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

5) Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.

6) Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.

7) Este interzisă instalarea programelor de tip shareware sau freeware, fără aprobarea administratorului sistemului informatic.

5.3. *Autorizarea accesului fizic:*

1) Accesul în sediile/oficiile/birourile ori spaţiile unde sunt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar angajaţilor Inspectoratului sau vizitatorilor care sunt legitimaţi în prealabil, şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare, pentru preîntâmpinarea accesului persoanelor neautorizate, fiind însoţiţi pe toata durata vizitei.

2) Accesul neautorizat în perimetrul de securitate a sediului Inspectoratului, unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video este interzis, ţinând cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de Legea privind protecţia datelor cu caracter personal şi Cerinţele fata de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale.

5.4. *Administrarea şi monitorizarea accesului fizic:*

1) Inspectoratul asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces. Înainte de acordarea accesului fizic la sistemele informaţionale şi/sau la registrele de date cu caracter personal, se verifica drepturile de acces ale fiecărui solicitant.

2) Perimetrul încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sunt rezistenţi, intrările sunt echipate cu lacăte şi/sau semnalizare. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii. Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

3) Sunt utilizate mijloace automatizate care asigură identificarea cazurilor de acces neautorizat şi iniţierea acţiunilor de blocare a accesului, precum şi de stocare a informaţiilor privind tentativele de acces neautorizat.

4) Accesul vizitatorilor (persoanelor terţe) se va asigura în conformitate cu regulile

prevăzute de legislaţia în vigoare cu privire la protecţia datelor cu caracter personal.

5) Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisa doar în cazul prezenţei unei permisiuni speciale a conducerii sau în conformitate cu procedura stabilită în Regulamentul privind supravegherea prin mijloace video.

5.5. *Asigurarea protecţiei datelor cu caracter personal:*

1) Salariaţii care în activitatea lor profesională intră în contact cu date considerate cu caracter personal sunt obligaţi să păstreze confidenţialitatea datelor şi să respecte întocmai prevederile cadrului normativ cu privire la protecţia datelor cu caracter personal.

2) Obligaţia privind păstrarea confidenţialităţii datelor cu caracter personal rămâne valabilă atât în cazul angajării sau transferării la un loc de muncă în cadrul Inspectoratului, precum şi după încetarea raportului de muncă.

3) Dispoziţiile prezentului articol se aplica, în acelaşi mod, pentru toate informaţiile deţinute de Inspectorat referitoare la terţi, despre care salariatul ia cunoştinţă în cadrul activităţii sale.

5.6. *Prelucrarea datelor cu caracter personal:*

1) Este interzisă prelucrarea datelor cu caracter personal fără consimţământul subiectului datelor cu caracter personal, cu excepţia cazurilor prevăzute de legislaţia în vigoare.

2) Politica de securitate, în mod obligatoriu va fi adusă la cunoştinţă, sub semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

3) La încheierea operaţiunilor de prelucrare a datelor cu caracter personal, dacă subiectul acestor date nu şi-a dat consimţământul pentru o altă destinaţie, pentru stocare sau pentru o prelucrare ulterioara, acestea vor fi distruse, transferate sau transformate şi stocate conform legislaţiei in vigoare.

5.7. *Identificarea şi autentificarea utilizatorilor:*

1) În cazul accesului la o bază de date deţinută pe un suport fizic, identificarea persoanei va fi efectuată de către persoana care deţine baza, cu înregistrarea obligatorie a numelui, prenumelui, funcţia, data şi scopul solicitării de acces.

2) Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal prelucrată în sistemele TI şi deţinută de Inspectorat, trebuie să se identifice. Identificarea se va face prin introducerea unui cont de utilizator (sau „user-name") şi a parolei asociate respectivului cont de utilizator (parola de peste 8 caractere ce va fi formată din mai multe tipuri de caractere, respectiv cifre, litere şi caractere speciale).Identificarea utilizatorilor se poate face prin introducerea codului de identificare de la tastatură (un sir de caractere).

3) Fiecărui utilizator ce i se va permite accesul la bazele de date cu caracter personal ale Inspectoratului va avea propriul său user-name şi parolă, care vor fi unice la nivelul Inspectoratului. Administrarea identificatorilor utilizatorilor include (i) identificarea

univoca a fiecărui utilizator, şi (ii) verificarea autenticităţii fiecărui utilizator.

4) User-name-urile nefolosite o perioadă mai îndelungata vor fi dezactivate şi distruse după un control prealabil intern al Operatorului. Această perioada după care conturile de utilizator vor fi dezactivate şi distruse este de maxim 90 de zile de la data ultimului acces (login) a respectivului utilizator. 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 perioada îndelungată, codurile de identificare şi autentificare se revocă sau se suspendă de administratorul TI.

5) Toţi utilizatorii se vor loga la bazele de date cu caracter personal ale Inspectoratului având în vedere faptul că sistemul informatic va refuza automat accesul utilizatorului la introducerea greşită a parolei.

6) Orice utilizator care primeşte un cont de utilizator şi o parolă asociată este obligat să respecte următoarele reguli:

- păstrarea confidenţialităţii stricte a acestora, în caz contrar urmând să răspundă în faţa Inspectoratului disciplinar, civil, penal etc., după caz, în conformitate cu legislaţia;
- interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;
- modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei;
- alegerea parolelor calitative cu o mărime de minimum 8 caractere, care nu sunt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sunt compuse integral din grupuri de cifre sau litere;
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

7) Inspectoratul administrează şi gestionează conturile de utilizator (şi implicit parolele asociate) ţinând cont de prezenta Politică.

8) Inspectoratul va autoriza doar anumiţi utilizatori pentru a revoca sau a suspenda un cont de utilizator şi parola asociată respectivului cont, dacă raporturile de serviciu cu utilizatorul au fost suspendate sau încetate, acesta a fost transferat în alt departament şi noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă a absentat o perioada îndelungata (mai mult de 3 luni).

9) Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste aprobate de persoana responsabilă din cadrul Inspectoratului.

10) Drepturile de acces ale utilizatorilor la bazele de date cu caracter personal sunt revizuite/controlate cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate şi/sau după oricare schimbare de statut al utilizatorului. Controlul sistematic al acţiunilor utilizatorilor este, de asemenea, efectuat în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

11) Accesul la funcţiile de securitate ale sistemelor informaţionale de date cu caracter personal şi la datele acestora este acordat în mod special doar persoanelor responsabile ale Operatorului, desemnate conform prevederilor prezentei Politici.

12) Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal, se blochează (la solicitarea utilizatorului sau în mod automat, după expirarea perioadei prestabilite de inactivitate a utilizatorului), fapt care face imposibil accesul de mai departe până în momentul când utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

5.8. *Identificarea si autentificarea echipamentului:*

Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal, cu menţinerea acestor informaţii pentru o perioada îndelungată.

5.9. *Controlul administrării accesului:*

Este efectuat controlul sistematic al acţiunilor utilizatorilor în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

5.10. *Tipurile de acces:*

5.10.1. Accesul de la distanţă:

1) Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizând-se VPN, criptarea, cifrarea etc.), precum şi sunt documentate, supuse monitorizării şi controlului.

2) Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este autorizată de persoanele responsabile ale Inspectoratului şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

3) Accesul fără fir la sistemele informaţionale de date cu caracter personal este limitat la maximum, 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 a Inspectoratului.

5.10.2. Administrarea accesului portativ şi mobil:

1) Pentru toate categoriile sistemelor informaţionale de date cu caracter personal sunt stabilite limitări şi sunt elaborate reguli de folosire a echipamentului portativ şi mobil care permit accesul la sistemele informaţionale de date cu caracter personal.

2) Accesul la sistemele informaţionale de date cu caracter personal cu folosirea echipamentului portativ şi mobil se documentează, este monitorizat şi controlat.

3) Folosirea echipamentului portativ şi mobil este autorizată de persoanele responsabile ale deţinătorului de date cu caracter personal.

5.11. *Securitatea electroenergetică:*

1) Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.

2) În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

3) Sunt implementate sisteme automatizate de depistare şi semnalizare a incendiilor în birourile unde sunt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

4) Sunt prevăzute surse alternative de alimentare cu energie electrica de scurtă durată, care sunt folosite pentru terminarea corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

5.12. *Controlul instalării şi scoaterii componentelor TI:*

1) Este exercitat controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program utilizate în cadrul sistemelor informaţionale de date cu caracter personal.

2) 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, evitându-se folosirea funcţiilor standarde de nimicire.

5.13. *Colectarea datelor cu caracter personal:*

1) Inspectoratul colectează datele cu caracter personal de la subiecţii datelor cu caracter personal, cu informarea acestora despre categoriile de date şi scopul prelucrării datelor cu caracter personal. În acest sens, fiecare subiect al datelor cu caracter personal îşi exprimă consimţământul conform legislaţiei în vigoare.

2) Utilizatorii autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional sunt desemnaţi de IPM.

3) Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizaţi desemnaţi de Operator. Sistemul informaţional va înregistra cine a făcut modificarea, data şi ora modificării.

4) Nomenclatorul datelor cu caracter personal este indicat de către Inspectorat în fiecare regulament care vizează sistemele notificate Centrului National pentru Protecţia Datelor cu Caracter Personal. În cazul prelucrării unor date cu caracter personal suplimentare, Inspectoratul va efectua modificările de rigoare în regulamentele sistemelor notificate, cu informarea Centrului National pentru Protecţia Datelor cu Caracter Personal.

5) Datele personale ale subiecţilor datelor cu caracter personal pot fi supuse următoarelor metode de prelucrare: colectare, înregistrare, organizare, stocare, păstrare, restabilire, adaptare ori modificare, extragere, consultare, utilizare, dezvăluire prin transmitere, diseminare sau în orice alt mod, alăturare ori combinare, blocare, ştergere sau distrugere, transmitere către autorităţile publice competente în conformitate cu legislaţia în vigoare şi transmitere transfrontalieră.

6) În conformitate cu prevederile legislaţiei în vigoare, subiectul datelor cu caracter personal este informat asupra drepturilor pe care le are în legătură cu prelucrarea datelor

sale personale, în special despre:

- dreptul de acces la datele cu caracter personal;
- dreptul de intervenţie asupra datelor cu caracter personal;
- dreptul de opoziţie al subiectului datelor cu caracter personal;
- dreptul de a nu fi supus unei decizii individuale;
- alte drepturi.

7) În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, este necesară informarea persoanei (exceptând cazul în care el deţine deja informaţiile respective) cu privire la:

- identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridica, IDNO-ul, numărul de înregistrare în Registrul de evidenta al operatorilor de date cu caracter personal);
- scopul concret al prelucrării datelor cu caracter personal colectate;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existenta drepturilor la informare şi de acces la datele colectate; de intervenţie asupra datelor (în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorita caracterului incomplet sau inexact al acestora) şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia.

8) Subiecţilor de date cu caracter personal le este asigurat dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţi subiecţi, conţinute în fişele personale (alte materiale), cu excepţia cazurilor în care solicitanţii îşi realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

9) Dreptul de informare este asigurat de către Inspectorat în calitate de operatorul datelor cu caracter personal (sau entităţile ce asigură mentenanţa sistemului Inspectoratului) tuturor persoanelor supuse prelucrării.

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

11) Inspectoratul va desemna utilizatorii autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional, urmând ca orice

modificare a datelor cu caracter personal să fie efectuată numai de către respectivii utilizatori autorizaţi desemnaţi de Inspectorat.

12) Sistemul informaţional din cadrul Inspectoratului înregistrează, în permanenţă, cine a făcut modificarea, data şi ora modificării şi asigură menţinerea în mod separat a datelor şterse sau modificate, fără ca acestea din urma să interfereze în vreun fel cu informaţiile actualizate.

13) Datele personale pot fi dezvăluite, în condiţiile legii, către subiecţii datelor cu caracter personal, autorităţi publice centrale/locale, servicii sociale sau de sănătate, reprezentanţii legali ai subiecţilor datelor cu caracter personal, alte entităţi care oferă garanţii suficiente de protecţie a datelor personale.

14) Prelucrarea datelor cu caracter personal de către Inspectorat va fi efectuată pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care acestea sunt prelucrate. După expirarea acestei perioade, datele cu caracter personal vor fi păstrate în formă arhivată în conformitate cu Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova, aprobat prin Ordinul nr.57 din 27.07.2016 al Serviciului de Stat de Arhiva.

5.14. *Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate:*

1) Stocarea şi păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sunt conectate la internet, nu sunt echipate cu mijloace de protecţie speciale tehnice şi de program şi nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii soft-ului, de asigurare a efectuării periodice a copiilor de siguranţa şi de efectuare a auditului - este interzisă.

2) Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredinţate doar persoanei responsabile desemnate din cadrul Inspectoratului.

3) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al Inspectoratului este interzisă.

5.15. *Dezvăluirea datelor cu caracter personal:*

1) Dezvăluirea informaţiilor ce conţin date cu caracter personal în format electronic conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată prin criptarea acestei informaţii sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidenţă a datelor cu caracter personal este permis doar utilizatorilor

autorizaţi. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronica va fi examinat separat, reieşind din posibilităţile tehnice asigurate de destinatar şi Inspectorat în calitate de operator de date cu caracter personal, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi. În cazul în care reţelele comunicaţionale prezinta riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmânarea personală, etc.).

2) Dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund Cerinţelor, (spre exemplu: expedierea informaţiei prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com) etc, sunt interzise, cu excepţia cazurilor în care are loc transmiterea datelor cu caracter personal în adresa subiectului de date.

3) Sunt interzise operaţiunile de dezvăluire a datelor cu caracter personal între Inspectorat şi alte entităţi care sunt amplasate geografic în stânga Nistrului care refuză să se supună juridic legislaţiei Republicii Moldova, reieşind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce tine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecţia datelor cu caracter personal.

4) Transmiterea transfrontaliera a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile Legii privind protecţia datelor cu caracter personal, în special în cazurile când tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

5) Volumul şi categoriile datelor cu caracter personal colectate în scopul ţinerii evidentei Inspectoratului, este limitat la strictul necesar pentru realizarea scopurilor declarate.

6) Accesul la sistemele informaţionale gestionate în cadrul Inspectoratului, din partea agenţilor constatatori pe marginea cauzelor contravenţionale, organelor de urmărire penală sau instanţelor de judecată, va fi permisă doar în cazul în care solicitarea va corespunde prevederilor şi procedurilor prevăzute de legislaţie.

5.16. *Computerele şi terminalele de acces:*

1) Computerele şi terminalele de acces la informaţiile stocate au bazele în camere restricţionate şi securizate, la care au acces doar angajaţii numiţi prin Ordinul Şefului Inspectoratului. Acestea sunt protejate prin parole, iar bazele de date electronice sunt păstrate pe servere independente, sigure, localizate în zone controlate şi protejate.

2) Accesul la computere/terminale se face pe baza combinaţiei user/parolă.

3) În cazul monitoarelor pe al căror ecran apar date cu caracter personal asupra cărora nu se acţionează o perioada de maxim 15 (cincisprezece) minute, sesiunea de lucru se închide automat.

5.17. *Auditul sistemelor informaţionale gestionate:*

1) Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:

- data şi timpul tentativei intrării/ieşirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.

2) 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:

- data şi timpul tentativei de obţinere a accesului (executate a operaţiunii),
- denumirea (identificatorul) aplicaţiei sau procesului, ori ID-ul utilizatorului,
- specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.),
- tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.),
- rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.

3) Este efectuată înregistrarea modificărilor drepturilor de acces (competentelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

- data şi timpul modificării competenţelor,
- ID-ul administratorului care a efectuat modificările,
- ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

5.17.1. 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:

- data şi timpul eliberării,
- denumirea informaţiei şi căile de acces la aceasta,
- specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic),
- ID-ul utilizatorului, care a solicitat informaţia.

5.18. *Asigurarea protecţiei contra programelor dăunătoare (viruşilor):*

Este asigurata protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existenta programelor licenţiate anti-virus.

5.19. *Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal:*

Se asigură testarea funcţionării corecte a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

5.20. *Gestionarea incidentelor de securitate:*

1) Personalul Inspectoratului informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

2) În cazul producerii incidentelor de securitate în cadrul Inspectoratului, persoana

responsabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului National pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova.

3) În cadrul controalelor efectuate de Centrul National pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova, angajaţilor acestuia li se vor oferi suportul necesar şi li se va asigura accesul la informaţiile necesare relevante obiectului controlului, conform prevederilor legale în vigoare.

4) Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent prin mijloace automatizate. Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

5) Personalul care asigura exploatarea sistemelor informaţionale de date cu caracter personal trece instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

6) Personalul Inspectoratului informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

7) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea, înlăturarea şi restabilirea securităţii.

8) Până la 31 ianuarie a fiecărui an, Inspectoratul informează în scris Centrul National pentru Protecţia Datelor cu Caracter Personal despre incidentele de securitate constatate.

5.21. *Responsabilitatea pentru asigurarea securităţii datelor cu caracter personal precum şi a informaţiilor cu accesibilitate limitata:*

1) Pentru nerespectarea prevederilor dispoziţiilor Politicii de securitate, persoanele vinovate sunt pasibile de răspundere civila, contravenţionala sau penală, după caz.

2) Drepturile subiecţilor de date cu caracter personal:

În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile Legii privind protecţia datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informaţii, exceptând cazul în care el deţine deja informaţiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator *(denumirea, adresa juridica, IDNO-ul)*;
- privind scopul concret al prelucrării datelor cu caracter personal colectate;
- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existenta drepturilor la informare şi de acces la datele colectate; de intervenţie asupra datelor *(în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora)* şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care

se colectează informaţia.

3) Subiecţilor de date cu caracter personal le este asigurat dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal vizate nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţi subiecţi, conţinute în fişele personale (alte materiale), cu excepţia cazurilor în care solicitanţii îşi realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

4) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entităţile ce asigura menţinerea sistemului) tuturor persoanelor supuse prelucrării.

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

Aprobat
prin Ordinul Şefului IPM
Nr. 14 din 01. 02. 2023

REGULAMENT
privind prelucrarea datelor cu caracter personal ale angajaţilor Inspectoratului pentru Protecţia Mediului şi altor persoane fizice în procesul de administrare a resurselor umane în cadrul Inspectoratului pentru Protecţia Mediului

I. Dispoziţii generale

1.1. Regulamentul privind protecţia datelor cu caracter personal ale angajaţilor (*în continuare Inspectorat, IPM*) şi altor persoane fizice în procesul de administrare a resurselor umane în cadrul Inspectoratului, constituie un ansamblu de mijloace organizaţionale ce asigură colectarea, transmiterea şi controlul datelor personale ale angajaţilor IPM, ale altor persoane fizice, realizarea proceselor de prelucrare, de analiză şi pregătire a informaţiei pentru gestionarea eficientă a resurselor umane din cadrul IPM şi pentru asigurarea normelor prevăzute de Legea nr.133/2011 privind protecţia datelor cu caracter personal, ale Hotărârii Guvernului nr.1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, inclusiv conform Instrucţiunii cu privire la asigurarea securităţii datelor cu caracter personal din cadrul Sistemului Informaţional Automatizat „Registrul funcţiilor publice şi al funcţionarilor publici" (în continuare RFPFP) a Cancelariei de Stat a Guvernului, ale anexei nr.11 la Hotărârea Guvernului nr.201/2009, prin care este aprobată Instrucţiunea cu privire la gestionarea dosarului personal al funcţionarului public, precum şi ale art.13 "Evidenţa funcţiilor publice şi ale funcţionarilor publici" din Legea nr.158/04.07.2008 cu privire la funcţia publică şi statutul funcţionarului public, ale Legii nr.133/2016 privind declararea averii şi a intereselor personale, ale Hotărârii Guvernului nr.673/2017 pentru implementarea legii menţionate, precum şi întru respectarea prevederilor art.91 – 94 ale Codului muncii al RM.

1.2. Prin prezentul Regulament sunt reglementate condiţiile generale şi cerinţele faţă de prelucrarea datelor cu caracter personal al angajaţilor Inspectoratului în cadrul sistemului de evidenţă a resurselor umane.

II. Abrevieri şi termenii folosiţi

2.1. Pe parcursul Regulamentului abrevierile semnifică:

SIA – Sistemul Informaţional Automatizat;

SIA RFPFP – Sistemul Informaţional Automatizat „Registrul funcţiilor publice şi al funcţionarilor publici";

SIA RESDAIP – Sistemul Informaţional Automatizat „ Registrul electronic al subiecţilor declarării averii şi a intereselor personale"

CM – Codul Muncii al RM.

2.2. Pe parcursul Regulamentului termenii au următorul sens după cum urmează:

date cu caracter personal – orice informaţie referitoare la angajatul IPM sau 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.

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.

organul de control al prelucrărilor de date cu caracter personal – Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova.

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.

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.

tehnologie informaţională (TI) – totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia.

utilizator – angajatul Secţiei resurse umane care acţionează sub autoritatea deţinătorului de date cu caracter personal, inclusiv cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal, prevăzute în mod expres de legislaţia în vigoare.

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 suport de hârtie şi pe suport informaţional a datelor cu caracter personal.

III. Scopul

3.1. Inspectoratul pentru Protecţia Mediului colectează în mod direct şi indirect date cu caracter personal ale angajaţilor IPM şi ale altor persoane fizice în procesul de administrare a resurselor umane şi le prelucrează, conform prevederilor Instrucţiunii cu privire la gestionarea dosarului personal al funcţionarului public, aprobat prin anexa nr.11 la Hotărârea Guvernului nr.201/20109 în următoarele scopuri:

– gestiunea resurselor umane în cadrul IPM, prin deţinerea informaţiilor despre angajaţi şi despre modul în care aceştia îşi exercită funcţia publică;

– evidenţa personalului care activează în cadrul IPM, inclusiv evidenţa funcţionarilor publici la nivel naţional, prin administrarea dosarelor personale ale acestora şi a SIA RFPFP al Cancelariei de Stat şi a SIA RESDAIP al Autorităţii Naţionale de Integritate;

– desfăşurarea concursurilor pentru ocuparea funcţiilor publice vacante;

– evidenţa funcţionarilor publici din cadrul IPM pentru depunerea Declaraţiei de avere şi interese personale, prin completarea şi actualizarea SIA RESDAIP al Autorităţii Naţionale de Integritate.

3.2. Prelucrarea datelor cu caracter personal care fac obiectul prelucrării trebuie să fie realizată cu respectarea următoarelor principii:

- prelucrate în mod corect şi conform prevederilor legii;
- colectate în scopuri determinate, explicite şi legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri;
- adecvate, pertinente şi neexcesive în ceea ce priveşte scopul pentru care sunt colectate şi/sau prelucrate ulterior;
- exacte şi, dacă este necesar, actualizate;
- 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 sunt colectate şi ulterior prelucrate;
- respectate drepturile subiectului de date cu caracter personal;
- asigurată confidenţialitatea şi respectate măsurile organizatorice şi tehnice de securitate necesare pentru protecţia datelor cu caracter personal.

IV. Drepturile persoanelor vizate

4.1. Inspectoratul în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecţia datelor cu caracter personal ce le revin angajaţilor, precum şi, după caz, altor persoane vizate.

4.2. În conformitate cu principiile de protecţie a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenţie, de opoziţie asupra datelor cu caracter personal ce-i vizează, precum şi dreptul de a se adresa în justiţie.

4.3. Secţia resurse umane ţine evidenţa personalului Inspectoratului, a datelor şi a documentelor cu privire la personalul IPM, administrează baza de date computerizată privind personalul IPM prin completarea SIA "Registrul funcţiilor publice şi al funcţionarilor publici", actualizează permanent SIA „Registrul electronic al subiecţilor declarării averii şi a intereselor personale" (în continuare SIA RESDAIP) cu datele referitoare la angajaţii Inspectoratului, asigură protecţia datelor cu caracter personal ale personalului, inclusiv şi a confidenţialităţii acestora, asigură administrarea personalului prin planificarea, coordonarea, organizarea, desfăşurarea, monitorizarea şi evaluarea implementării în cadrul IPM a procedurilor de personal.

4.4. Pentru executarea prezentului Regulament responsabili se desemnează :

4.4.1. Angajaţii Secţiei resurse umane din cadrul Inspectoratului - de prelucrarea datelor cu caracter personal ale angajaţilor şi altor persoane fizice în procesul de administrare a resurselor umane în cadrul IPM, desemnaţi prin Ordinul şefului IPM, care asigură :

- implementarea prevederilor politicii de securitate a datelor cu caracter personal ale angajaţilor şi altor persoane fizice în procesul de administrare a resurselor umane în cadrul IPM;
- măsurile organizaţionale pentru protecţia datelor cu caracter personal;
- controlul accesului funcţionarilor din cadrul IPM la datele cu caracter personal, reieşind din atribuţiile lor funcţionale;
- identificarea riscurilor aferente prelucrării datelor cu caracter personal şi măsurilor de minimizare a acestora;
- completarea şi semnarea ***Acordului*** privind prelucrarea datelor cu caracter personal ale angajatului Inspectoratului, inclusiv prin intermediul SIA RFPFP şi prin intermediul SIA RESDAIP de către angajaţii IPM, inclusiv de către noii angajaţi sau reîncadraţi în funcţie în cadrul IPM, conform anexei nr.1 a Regulamentului;
- completarea şi semnarea ***Angajamentului*** privind păstrarea confidenţialităţii datelor cu caracter personal ale angajaţilor Inspectoratului, de către angajaţii Secţiei resurse umane, inclusiv de către noii angajaţi sau reîncadraţi în funcţie ai acestei subdiviziuni, conform anexei nr.2 a Regulamentului;
- completarea şi semnarea ***Angajamentului*** privind păstrarea confidenţialităţii datelor cu caracter personal ale angajaţilor Inspectoratului, precum şi a informaţiilor ce ţin de salarizare de către angajaţii Direcţiei finanţe şi logistică, inclusiv şi de către noii angajaţi sau reîncadraţi în funcţie ai acestei subdiviziuni, conform anexei nr.3 a Regulamentului;

- anexarea actelor semnate (Anexele nr.1, nr.2 şi nr.3 ale Regulamentului) la dosarele personale ale angajaţilor respectivi.

4.4.2. Şeful Secţiei resurse umane a Inspectoratului, asigură:

- organizarea corectă a procesului de prelucrare a documentelor şi de asigurare a securităţii datelor cu caracter personal, prelucrate în cadrul subdiviziunii în gestiune;
- crearea condiţiilor administrativ-organizatorice , orientate spre protejarea datelor cu caracter personal împotriva accesului neautorizat, distrugerii, modificării, blocării, copierii sau difuzării acestora, precum şi a altor acţiuni ilegale cu asemenea date;
- protecţia documentelor, inclusiv a dosarelor personale ale angajaţilor Inspectoratului şi altor purtători de date cu caracter personal, prin păstrarea acestora în locuri sigure, care să prevină accesul neautorizat (safeuri/dulapuri metalice cu cheie, încăperi de arhivă);
- evidenţa, păstrarea, arhivarea şi nimicirea informaţiilor care conţin date cu caracter personal cu menţinerea înregistrărilor respective;
- înştiinţarea persoanei responsabile de politica de securitate a datelor cu caracter personal despre orice fapt de incidente/suspiciuni de încălcare a securităţii datelor cu caracter personal.
- coordonarea cu persoana responsabilă de politica de securitate a datelor cu caracter personal, la transmiterea sau diseminarea datelor cu caracter personal pe extern.

4.4.3. Persoanele implicate în prelucrarea datelor cu caracter personal (angajaţii Secţiei resurse umane - utilizatorii ai SI), asigură:

- confidenţialitatea şi integritatea prelucrării datelor cu caracter personal cu respectarea prevederilor actelor legislative şi normative în domeniul prelucrării şi asigurării securităţii datelor cu caracter personal, inclusiv procedurilor interne şi măsurilor de protecţie stipulate în prezentul Regulament;
- securitatea datelor împotriva accesului nesancţionat, distrugerii, modificării, blocării, copierii sau difuzării acestora, precum şi a altor acţiuni ilegale cu asemenea date;
- semnarea şi respectarea clauzelor de confidenţialitate, stabilite conform prevederilor interne (contract de confidenţialitate).

4.5. Datele cu caracter personal deţinute în vederea prelucrării în dosarul personal, după caz şi în cadrul SIA sunt următoarele:

- numele, prenumele, patronimicul;
- seria şi numărul din buletinul de identitate/permisul de şedere/paşaport;
- data şi locul naşterii;
- adresa (domiciliul/reşedinţa);
- adresa e-mail;
- numărul de telefon;
- date privind plăţile salariale;
- seria, numărul diplomei de studii, studiile deţinute.

4.6. Dreptul de acces la dosarul personal îl are:

- Funcţionarul public, ca urmare a unei solicitări verbale adresate şefului Secţiei resurse umane, care se consemnează în fişa de evidenţă a persoanelor care au avut acces la dosarul personal;

- Şeful IPM, Şefii adjuncţi a IPM, şeful Serviciului audit şi securitate internă sau şefii subdiviziunilor structurale în care îşi desfăşoară activitatea funcţionarul public ca urmare a unei solicitări verbale adresate şefului Secţiei resurse umane, care se consemnează în fişa de evidenţă a persoanelor care au avut acces la dosarul personal;

4.7. Funcţionarul public are dreptul, la cererea verbală sau scrisă adresată şefului Secţiei resurse umane, de a primi:

- copii simple de pe documentele din dosarul său personal sau certificate prin ştampilă şi semnătură de către şeful Secţiei resurse umane;

- extrase de pe documentele întocmite, certificate prin ştampilă şi semnătură de către şeful Secţiei resurse umane;

- adeverinţe care atestă informaţii cuprinse în dosarul său personal.

4.8. Copiile, extrasele şi adeverinţele menţionate la pct.9 şi 10 pot fi obţinute şi de către alte persoane sau instituţii în limita cadrului legal.

4.9. În adresările/ răspunsurile care conţin date cu caracter personal se va specifica menţiunea „Suportul conţine date cu caracter personal şi sunt permise spre utilizare doar destinatarului. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de legislaţie".

V. Măsurile de protecţie a datelor cu caracter personal prelucrate şi stocate în cadrul Inspectoratului

5.1. Încăperile unde se efectuează prelucrarea datelor cu caracter personal sunt dotate cu safeuri/dulapuri metalice, la care au acces doar şeful Secţiei resurse umane şi persoanele cu atribuţii în domeniul gestionării resurselor umane, inclusiv a dosarelor personale, dotate cu mijloace tehnice de securitate ce asigură siguranţa suporturilor de date, restricţionarea accesului persoanelor neautorizate, precum şi controlul vizual al persoanelor amplasate în aceste încăperi.

5.2. Toate dosarele personale ale angajaţilor IPM se păstrează în safeuri sau dulapuri metalice.

5.3. Se interzice scoaterea dosarelor personale din încăperile unde se păstrează, cu excepţia prevederilor cadrului legal.

5.4. Dosarul personal al funcţionarului public al cărui raport de serviciu a încetat, se transmite conform cadrului legal în arhiva Inspectoratului sau autorităţii publice respective în cazul transferului/promovării funcţionarului public în altă autoritate publică.

5.5. Măsurile generale de administrare a securităţii informaţionale:

5.5.1 În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie care conţin date preluate din sistemul de evidenţă, aceştia se păstrează în safeuri

care se încuie.

5.5.2 La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la reţeaua electrică.

5.5.3 Operatorul asigură securitatea punctelor de primire şi expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.

5.5.4 Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidenţă este blocat împotriva vizualizării de către persoane neautorizate.

5.5.5 Mijloacele de prelucrare a informaţiilor preluate din sistemul de evidenţă sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

5.5.6 Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidenţă din/în perimetrul de securitate se înregistrează în registru.

5.6. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidenţă, se înfăptuiesc ţinând cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală.

5.7. Accesul în birourile Inspectoratului este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program.

5.8. Biroul nu este lăsat niciodată fără supraveghere la ieşirea în exterior.

5.9. Înainte de acordarea accesului fizic la sistemul de evidenţă, se verifică competenţele de acces.

5.10. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

5.11. Perimetrul de securitate se consideră perimetrul birourilor în care este amplasat sistemul de evidenţă, fiind integre din punct de vedere fizic, acestea zilnic, se inspectează sub aspectul integrităţii.

5.12. Accesul persoanelor neautorizate în cadrul perimetrelor de securitate va fi chestionat pentru a evita accesul neautorizat şi fiecare situaţie va fi raportată persoanelor responsabile cu acordarea drepturilor de acces şi asigurarea securităţii.

5.13. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine.

5.14. Amplasarea sistemului de evidenţă răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

5.15. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă , a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. In cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemul de evidenţă, inclusiv posibilitatea

deconectării oricărui component TI.

5.16. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor, sunt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaționale.

5.17. Controlul instalării și scoaterii componentelor TI: se efectuează controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemului de evidență. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

VI. Durata de stocare

6.1. Prelucrarea datelor cu caracter personal în sistemul de evidență a resurselor umane se efectuează pe perioada activității angajaților Inspectoratului, valabilității relațiilor de muncă, contractelor individuale de muncă (din momentul angajării până la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

6.2. Datele cu caracter personal a potențialilor salariați se preia din CV-ul transmis de către aceştia la adresa de e-mail a subdiviziunii responsabile de resursele umane. După primirea CV-ului prin intermediul poştei electronice, acesta se tipăreşte pe suport de hârtie, iar de pe adresa de e-mail se şterge conținutul mesajului. Totodată, în cazul în care potențialii salariați nu au fost admişi la funcția vacantă din cadrul Inspectoratului, atunci persoana responsabilă de sistemul de evidență a resurselor umane distruge CV-urile potențialilor angajați.

6.3. La expirarea termenelor menționate în punctul 6.1., datele din sistemul de evidență a resurselor umane sunt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul dosarelor aprobat prin Ordinul Inspectoratului sau Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile şi întreprinderile Republicii Moldova, aprobat de Agenția Națională a Arhivelor nr.57 din 27.07.2016, ulterior fiind supuse distrugerii sau ştergerii, în funcție de suportul pe care au fost efectuate.

VII. AUDITUL SECURITĂȚII ÎN SISTEMUL DE EVIDENȚĂ A RESURSELOR UMANE

7.1. Se organizează generarea înregistrărilor de audit a securității în sistemul de evidență pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

7.2. înregistrările de audit a securității sistemului de evidență în care sînt prelucrate date cu caracter personal, trebuie să conțină:

- numele şi prenumele utilizatorului;
- numele fişei accesate (pagina şi inscripția din registru);
- numărul înregistrărilor efectuate;
- tipul de acces;

- data accesului (an, lună, zi);
- timpul (ora, minuta) şi durataaccesului.

7.3. Rezultatele auditului securităţii în sistemul de evidenţă (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.

7.4. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidenţă constituie 2 */doi/* ani, în scopul asigurării posibilităţii de folosire a 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.

VIII. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENŢĂ A RESURSELOR UMANE

8.1. Persoanele care asigură exploatarea sistemului de evidenţă trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

8.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidenţă.

8.3. În cazul producerii incidentelor de securitate persoanele responsabile vor întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate.

8.4. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din sistemul de evidenţă a resurselor umane poartă răspundere pentru acţiunile sale.

IX. SPECIFICUL LEGISLAŢIEI MUNCII PRIVIND PRELUCRAREA DATELOR PERSONALE ALE SALARIAŢILOR

9.1. În conformitate cu art.91 al CM, angajatorul şi reprezentanţii lui sunt obligaţi să respecte următoarele cerinţe:

a) prelucrarea datelor personale ale salariatului poate fi efectuată exclusiv în scopul îndeplinirii prevederilor legislaţiei în vigoare, acordării de asistenţă la angajare, instruirii şi avansării în serviciu, asigurării securităţii personale a salariatului, controlului volumului şi calităţii lucrului îndeplinit şi asigurării integrităţii bunurilor unităţii;

b) la determinarea volumului şi conţinutului datelor personale ale salariatului ce urmează a fi prelucrate, angajatorul este obligat să se conducă de legislaţia în vigoare;

c) toate datele personale urmează a fi preluate de la salariat sau din sursa

indicată de acesta;

d) angajatorul nu este în drept să obţină şi să prelucreze date referitoare la convingerile politice şi religioase ale salariatului, precum şi la viaţa privată a acestuia. în cazurile prevăzute de lege, angajatorul poate cere şi prelucra date despre viaţa privată a salariatului numai cu acordul scris al acestuia;

e) angajatorul nu este în drept să obţină şi să prelucreze date privind apartenenţa salariatului la sindicate, asociaţii obşteşti şi religioase, partide şi alte organizaţii social-politice, cu excepţia cazurilor prevăzute de lege;

f) la adoptarea unei decizii care afectează interesele salariatului, angajatorul nu este în drept să se bazeze pe datele personale ale salariatului obţinute exclusiv în urma prelucrării automatizate sau pe cale electronică;

g) protecţia datelor personale ale salariatului contra utilizării ilegale sau pierderii este asigurată din contul angajatorului;

h) salariaţii şi reprezentanţii lor trebuie să fie familiarizaţi, sub semnătură, cu documentele vizând modul de prelucrare şi păstrare a datelor personale ale salariaţilor din unitate şi să fie informaţi despre drepturile şi obligaţiile lor în domeniul respectiv;

i) salariaţii nu trebuie să renunţe la drepturile lor privind păstrarea şi protecţia datelor personale;

j) angajatorii, salariaţii şi reprezentanţii lor trebuie să elaboreze în comun măsurile de protecţie a datelor personale ale salariaţilor.

9.2. Conform art.92 al CM, la transmiterea datelor personale ale salariatului, angajatorul trebuie să respecte următoarele cerinţe:

a) să nu comunice unor terţi datele personale ale salariatului fără acordul scris al acestuia, cu excepţia cazurilor când acest lucru este necesar în scopul prevenirii unui pericol pentru viaţa sau sănătatea salariatului, precum şi a cazurilor prevăzute de lege;

b) să nu comunice datele personale ale salariatului în scopuri comerciale fară acordul scris al acestuia;

c) să prevină persoanele care primesc datele personale ale salariatului despre faptul că acestea pot fi utilizate doar în scopurile pentru care au fost comunicate şi să ceară persoanelor în cauză confirmarea în scris a respectării acestei reguli. Persoanele care primesc datele personale ale salariatului sunt obligate să respecte regimul de confidenţialitate, cu excepţia cazurilor prevăzute lege;

d) să permită accesul la datele personale ale salariatului doar persoanelor împuternicite în acest sens, care, la rândul lor, au dreptul să solicite numai datele personale necesare exercitării unor atribuţii concrete;

e) să nu solicite informaţii privind starea sănătăţii salariatului, cu excepţia datelor ce vizează capacitatea salariatului de a-şi îndeplini obligaţiile de muncă;

f) să transmită reprezentanţilor salariaţilor datele personale ale salariatului în modul prevăzut de prezentul cod şi să limiteze această informaţie numai la acele date personale care sunt necesare exercitării de către reprezentanţii respectivi a atribuţiilor

lor.

9.3. Conform art.93 al CM, în scopul asigurării protecţiei datelor sale personale care se păstrează la angajator, salariatul are dreptul:

a) de a primi informaţia deplină despre datele sale personale şi modul de prelucrare a acestora;

b) de a avea acces liber şi gratuit la datele sale personale, inclusiv dreptul la copie de pe orice act juridic care conţine datele sale personale, cu excepţia cazurilor prevăzute de legislaţia în vigoare;

c) de a-şi desemna reprezentanţii pentru protecţia datelor sale personale;

d) de a avea acces la informaţia cu caracter medical ce-l vizează, inclusiv prin intermediul lucrătorului medical, la alegerea sa;

e) de a cere excluderea sau rectificarea datelor personale incorecte şi/sau incomplete, precum şi a datelor prelucrate cu încălcarea cerinţelor prezentului cod. în cazul în care angajatorul refuză să excludă sau să rectifice datele personale incorecte, salariatul este în drept să notifice în scris angajatorului dezacordul său motivat;

f) de a ataca în instanţa de judecată orice acţiuni sau inacţiuni ilegale ale angajatorului admise la obţinerea, păstrarea, prelucrarea şi protecţia datelor personale ale salariatului

X. DISPOZIŢII FINALE

10.1. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea Inspectoratului periodic, însă cel puţin o dată la doi ani, precum şi la necesitate.

10.2. Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

10.3. Regulamentul este adus la cunoştinţa angajaţilor prin comunicare directă sau prin publicarea pe pagina de web a Inspectoratului. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.

Anexa nr.1
la Regulamentul privind prelucrarea datelor cu caracter personal ale angajaţilor şi altor persoane fizice în procesul de administrare a resurselor umane în cadrul IPM, aprobat prin Ordinul Şefului IPM nr. ___ din „___”_____2023

ACORD

privind prelucrarea datelor cu caracter personal ale angajatului Inspectoratului pentru Protecţia Mediului, inclusiv prin intermediul SIA „Registrul funcţiilor publice şi al funcţionarilor publici” şi SIA „Registrul electronic al subiecţilor declarării averii şi a intereselor personale”

Subsemnatul/a _____ **IDNP** _____
Buletin de identitate Seria/nr. _____ **Data eliberării** _____, **Oficiul** _____

prin acest acord:

-*îmi exprim în mod expres consimţământul* neviciat la prelucrarea datelor cu caracter personal, care sunt oferite de mine Inspectoratului pentru Protecţia Mediului în scopul executării raporturilor mele de serviciu/de muncă apărute în baza actului administrativ de numire în funcţia publică/de angajare, inclusiv la colectarea şi prelucrarea acestora de către Inspectorat pe durata raporturilor de serviciu în SIA RFPFP, în scopul ţinerii evidenţei datelor şi documentelor cu privire la personalul autorităţii publice, inclusiv celor privind salarizarea mea şi înregistrarea informaţiilor contabile;

-*confirm că am fost informat/ă* cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal şi privind prelucrarea datelor cu caracter personal ce mă vizează.

_____ (Nume, prenume)	_____Semnătura _____Data

Prezentul acord a fost întocmit în două exemplare, câte unul pentru fiecare parte.

Am primit un exemplar	_____Semnătura

Atenţie! Suportul conţine date cu caracter personal şi sunt permise spre utilizare doar destinatarului. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal.

Anexa nr.2
la Regulamentul privind prelucrarea datelor cu caracter personal ale angajaţilor şi altor persoane fizice în procesul de administrare a resurselor umane în cadrul IPM, aprobat prin Ordinul Şefului IPM nr. ___ din „___”_____2023

ANGAJAMENT

privind păstrarea confidenţialităţii datelor cu caracter personal ale angajaţilor Inspectoratului pentru Protecţia Mediului, de către angajaţii Secţiei resurse umane

Subsemnatul/a _____, angajat/angajată în cadrul Inspectoratului pentru Protecţia Mediului, **în funcţia de** _____

mă oblig, în conformitate cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal şi ale Hotărârii Guvernului nr.1123/2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal”, să păstrez confidenţialitatea datelor cu caracter personal ale angajaţilor IPM, să respect măsurile tehnice şi organizatorice, necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate, inclusiv şi în cadrul Sistemului informaţional automatizat „Registrul funcţiilor publice şi al funcţionarilor publici”.

Data _____ Semnătura_____

Anexa nr.3

la Regulamentul privind prelucrarea datelor cu caracter personal ale angajaţilor şi altor persoane fizice în procesul de administrare a resurselor umane în cadrul IPM,

aprobat prin Ordinul Şefului IPM nr. ___ din „___” _____2023

ANGAJAMENT

privind păstrarea confidenţialităţi datelor cu caracter personal ale angajaţilor Inspectoratului pentru Protecţia Mediului, precum şi a informaţiilor ce ţin de salarizare de către angajaţii Direcţiei finanţe şi logistică

Subsemnatul/a _____, angajat/angajată în cadrul Inspectoratului pentru Protecţia Mediului, în funcţia de _____

mă oblig, în conformitate cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal şi ale Hotărârii Guvernului nr.1123/2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal”, să păstrez confidenţialitatea datelor cu caracter personal ale angajaţilor IPM, să respect măsurile tehnice şi organizatorice, necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate, precum şi a informaţiilor ce ţin de salarizare, inclusiv şi în cadrul Sistemelor informaţionale automatizate gestionate.

Data _____ Semnătura_____

APROBAT
prin Ordinul Şefului IPM
nr. 14 din 01.02.2023

L.Ş

REGULAMENTUL
privind prelucrarea datelor cu caracter personal în sistemul de evidenţă contabilă a Inspectoratului pentru Protecţia Mediului

I. DISPOZIŢII GENERALE

1.1. Regulamentul privind prelucrarea datelor cu caracter personal în sistemul de evidenţă contabilă a Inspectoratului pentru Protecţia Mediului *(în continuare - Regulament)* este elaborat în vederea implementării prevederilor Legii nr.133/2011 privind protecţia datelor cu caracter personal, Legii contabilităţii nr.113/2007 şi a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123/2010, precum şi întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condiţiile generale şi cerinţele faţă de prelucrarea datelor cu caracter personal ale angajaţilor Inspectoratului pentru Protecţia Mediului *(în continuare - Inspectorat)* în cadrul sistemului de evidenţă contabilă.

II. SCOPUL

2.1. Scopul prelucrării informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă contabilă constă în asigurarea înregistrării informaţiilor contabile referitoare la calculul drepturilor salariale ale angajaţilor, inclusiv a premiilor, stimulărilor, sporurilor, indemnizaţiilor, compensaţiilor şi altor drepturi şi obligaţii cu conţinut pecuniar, precum şi a prezentării rapoartelor financiare, trimestriale şi anuale către instituţiile statului, conform legislaţiei în vigoare.

2.2. În cadrul sistemului de evidenţă contabilă sunt prelucrate următoarele categorii de date cu caracter personal:

a) numele, prenumele şi patronimicul;

b) numărul personal de identificare de stat (IDNP);

c) data naşterii şi domiciliul;

d) codul personal de asigurări sociale (CPAS);

e) datele privind locul de muncă şi funcţia ocupată;

f) mărimea salariului brut şi alte premii, sporuri, stimulări, suplimente;

g) datele privind situaţia familială (la cererea solicitantului);

h) numele, prenumele (după caz, patronimicul) persoanelor care se află la întreţinerea persoanei respective (membrii familiei, alte rude şi persoane, după caz);

i) datele pentru transferul pe contul bancar a plăţilor salariale şi a altor sume datorate cu titlu de indemnizaţii, compensaţii sau alte beneficii, după caz;

j) datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizaţiei corespunzătoare;

k) mărimea concretă a drepturilor salariale calculate, taxele şi impozitele aferente, inclusiv contribuţiile de asigurări sociale obligatorii de asistenţă medicală şi socială, şi alte sume datorate în virtutea legii sau contractului;

l) după caz, alte date necesare îndeplinirii scopului menţionat, conform legislaţiei în vigoare.

2.3. Prelucrarea datelor cu caracter personal menţionate va fi efectuată pentru realizarea următoarelor scopuri:

a) Prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajaţii şi care au impact asupra calculării plăţilor salariale, de exemplu: modificarea gradului de calificare a funcţionarilor publici, avansarea în treptele de salarizare, acordarea sau retragerea dreptului de acces la secret de stat, evaluarea performanţelor profesionale cu acordarea sporului pentru performanţă, vechimea în muncă în serviciul public;

b) Calcularea salariilor lunare, în conformitate cu legislaţia în vigoare a Republicii Moldova (Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar);

c) Prelucrarea certificatelor de concedii medicale ale angajaţilor în vederea stabilirii indemnizaţiilor corespunzătoare;

d) Prelucrarea copiilor ordinelor conducerii Inspectoratului referitoare la personal;

e) Calcularea şi reţinerea taxelor ce ţin de plăţile salariale aferente angajaţilor: primele de asigurare obligatorie de asistenţă medicală, contribuţiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.;

f) Calcularea şi virarea primelor de asigurare obligatorie de asistenţă medicală şi a contribuţiilor la bugetul asigurărilor sociale de stat, aferente plăţilor salariale - obligaţie a angajatorului;

g) Furnizarea informaţiei necesare pentru elaborarea rapoartelor lunare privind contribuţiile de asigurare socială de stat obligatorii şi primele de asigurare obligatorie de asistenţă medicală (forma IPC 21) pentru fiecare angajat şi transmiterea acestora în format electronic prin SIA E-REPORTING şi anual.

h) Furnizarea informaţiei pentru stabilirea drepturilor sociale şi medicale a tuturor angajaţilor aferente raporturilor de muncă - IRM-19;

i) Asistarea procesului (prin furnizarea informaţiei necesare) pentru completarea periodică (lunară) a raportului şi dării de seamă privind venitul achitat şi impozitul pe venit reţinut din acesta;

j) Completarea lunară şi anuală a dărilor de seamă cu prezentarea acestora Serviciului Fiscal de Stat (privind impozitul pe venit IPC 21, TFD 19, IALS 18), precum şi perfectarea

şi eliberarea informaţiei privind veniturile calculate şi achitate în folosul persoanei fizice şi impozitul pe venit reţinut din aceste venituri angajaţilor Inspectoratului;

k) Prelucrarea cererilor şi a documentelor confirmative privind acordarea scutirilor la impozitul pe venit reţinut din salariu, în conformitate cu capitolul 4, titlul II din Codul Fiscal;

l) Eliberarea certificatelor de salariu, la cererea angajaţilor;

m) Completarea şi stocarea fişelor personale de evidenţă a veniturilor sub formă de salariu şi alte plăţi efectuate de către patron în folosul angajatului pe fiecare an, precum şi a impozitului pe venit reţinut din aceste plăţi (Anexa nr.8 la Ordinul IFPS nr.676/2007).

2.4. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/şterge, în funcţie de suportul pe care au fost efectuate. În cazul obligaţiilor expres prevăzute de lege acestea pot rămâne la păstrare primind statut de document de arhivă.

2.5. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidenţă contabilă în alte scopuri decât cele menţionate mai sus este interzisă.

III. LOCAŢIA ŞI DESCRIEREA SISTEMULUI DE EVIDENŢĂ CONTABILĂ

3.1. Datele cu caracter personal conţinute în sistemul de evidenţă contabilă în cadrul Inspectoratului se prelucrează/stochează:

1) pe suport de hârtie;

2) în format electronic:

a) Software – Sistemul de evidenţă contabilă în sfera bugetară 1C:Enterprise 8.3., care este instalat la 6 computere din sediul Inspectoratului pe adresa mun. Chişinău, str. Şos. Hînceşti, 53;

b) Hardware – calculator nr de inventariere 31460145.

3.2. Mentenanţa programului contabil 1C: Enterprise 8.3 este efectuată de către compania selectată în modul stabilit, fiind încheiat anual contract de valoare mică privind prestarea serviciilor de deservire între Inspectorat şi compania respectivă, cu următoarele atribuţii stabilite companiei prestatoare:

a) Efectuarea ajustărilor în program, în baza modificărilor legislaţiei Republicii Moldova;

b) Eliminarea erorilor în funcţionarea programului;

c) Consultarea în rezolvarea dificultăţilor apărute în utilizarea programului (Linia fierbinte);

d) Examinarea solicitărilor parvenite din partea Inspectoratului;

e) Examinarea bazei de date a Inspectoratului (la necesitate);

f) Vizite la faţa locului, la solicitarea Inspectoratului;

g) Examinarea şi nedivulgarea informaţiei cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

3.3. Prelucrarea informaţiilor în sistemul de evidenţă contabilă pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri;

IV. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidenţă contabilă se efectuează pe perioada activităţii angajaţilor Inspectoratului (din momentul semnării Ordinului de numire/contractului pînă la finalizarea efectuării acţiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă), pe perioada valabilităţii contractelor de achiziţie publică etc..

4.2. La expirarea termenelor menţionate în punctul 4.1., datele din sistemul de evidenţă contabilă sunt păstrate în formă arhivată, pe perioada stabilită de Inspectorat în Nomenclatorul dosarelor din cadrul Inspectoratului, ulterior fiind supuse distrugerii sau ştergerii, în funcţie de suportul pe care au fost efectuate.

V. DREPTURILE ANGAJAŢILOR ŞI PERSOANELOR VIZATE

5.1. Inspectoratul, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecţia datelor cu caracter personal ce le revin angajaţilor, precum şi, după caz, altor persoane vizate.

5.2. În conformitate cu principiile de protecţie a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenţie, de opoziţie asupra datelor cu caracter personal ce-i vizează, precum şi dreptul de a se adresa în justiţie.

5.3. Toate persoanele implicate în activitatea de administrare şi/sau prelucrare a informaţiilor din sistemul de evidenţă contabilă vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaţilor la informaţiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii Inspectoratului. Informaţiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum şi perioada concretă pentru care solicită informaţiile.

5.5. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informaţiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

VI. MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENŢĂ CONTABILĂ

6.1. Măsurile generale de administrare a securităţii informaţionale:

a) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronic care conţin date preluate din sistemul de evidenţă contabilă, aceştia se păstrează în safeuri care se încuie.

b) La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la reţeaua electrică.

c) Operatorul asigură securitatea punctelor de primire şi expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.

d) Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidenţă contabilă este blocat împotriva vizualizării de către persoane neautorizate.

e) Mijloacele de prelucrare a informaţiilor preluate din sistemul de evidenţă contabilă sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

f) Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidenţă contabilă din/în perimetrul de securitate se înregistrează în registru.

6.2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidenţă contabilă, se înfăptuiesc ţinând cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică şi externă.

6.3. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă contabilă, care conţin date cu caracter personal, sunt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspândirea acestora.

6.4. Accesul în biroul unde este amplasat sistemul de evidenţă contabilă este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi cheia de la lacătul mecanic.

6.5. Biroul nu este lăsat niciodată fără supraveghere la ieşirea în exterior, uşa, ferestrele biroului se încuie cu lacătul.

6.6. Înainte de acordarea accesului fizic la sistemul de evidenţă contabilă, se verifică competenţele de acces.

6.7. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

6.8. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidenţă contabilă, fiind integru din punct de vedere fizic, acesta zilnic, se inspectează sub aspectul de integritate.

6.9. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine.

6.10. Amplasarea sistemului de evidenţă contabilă răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

6.11. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă contabilă, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele de evidenţă contabilă, inclusiv posibilitatea deconectării oricărui component TI.

6.12. Computerele, unde este amplasat fizic sistemul de evidenţă contabilă, dispun de UPS-uri, care sunt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

6.13. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă contabilă, sunt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaţionale.

6.14. Securitatea anti incendiară a sistemului de evidenţă contabilă: biroul unde este amplasat sistemul de evidenţă contabilă este dotat cu echipament anti incendiar şi corespunde cerinţelor şi normelor anti incendiare în vigoare.

6.15. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidenţă contabilă. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

VII. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENŢĂ CONTABILĂ

7.1. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemele de evidenţă contabilă şi a proceselor executate în numele acestor utilizatori.

7.2. Toţi utilizatorii (inclusiv personalul care asigură mentenanţa tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului).

7.3. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lângă cerinţele de păstrare a confidenţialităţii parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepţia cazului de asigurare a securităţii păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

7.4. Se efectuează modificarea parolelor de fiecare dată când sunt depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.

7.5. Întru asigurarea posibilităţii de stabilire a responsabilităţii fiecărui utilizator, sunt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de

evidenţă a introducerilor greşite ale acestora. După trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.

7.6. Se asigură, pentru o perioadă de 1 */un/* an, păstrarea istoriilor anterioare ale parolelor în formă de cash a utilizatorilor şi prevenirea folosirii repetate a acestora.

7.7. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizaţii de acces primite în scopul comiterii unei fapte prejudiciabile, absenţă a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi autentificare se revocă sau se suspendă.

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidenţă contabilă, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidenţă contabilă, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 */una/* lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informaţiile din sistemul de evidenţă contabilă. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

7.9. În scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidenţă contabilă.

7.10. Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autorizează de persoanele responsabile de domeniul IT.

7.11. Se impun limite în privinţa persoanelor care au dreptul:

a) să vizualizeze informaţiile stocate în sistemul de evidenţă contabilă;

b) să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

7.12. Toţi angajaţii cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor cu caracter personal.

7.13. Orice activitate de dezvăluire a datelor cu caracter personal către terţi este documentată şi supusă unei analize riguroase în prealabil privind scopul şi temeiul legal a intenţiilor de dezvăluire a unui anumit volum de date cu caracter personal.

7.14. Orice încălcare a securităţii în ceea ce priveşte sistemul de evidenţă contabilă este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

7.15. Înainte de acordarea accesului în sistem, utilizatorii sunt informaţi despre faptul că folosirea sistemului de evidenţă contabilă este controlată şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia în vigoare.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE DE EVIDENŢĂ CONTABILĂ

8.1. Se organizează generarea înregistrărilor de audit a securităţii în sistemul de evidenţă contabilă pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

8.2. 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.

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării informaţiilor din sistemele de evidenţă contabilă, 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 al procesului;
c) ID-ul utilizatorului;
d) rezultatul tentativei de pornire – pozitivă sau negativă.

8.4. Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informaţiilor din sistemul de evidenţă contabilă, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau a 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.

8.5. Se efectuează 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.

8.6. Se efectuează înregistrarea ieşirii din sistemul de evidenţă contabilă, 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, filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

8.7. Cazurile de deranjament al auditului securităţii în sistemul de evidenţă contabilă sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sunt aduse la cunoştinţa persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

8.8. Rezultatele auditului securităţii în sistemul de evidenţă contabilă (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.

8.9. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidenţă contabilă constituie 2 */doi/* ani, în scopul asigurării posibilităţii de folosire a 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 INFORMAŢIILOR DIN SISTEMUL DE EVIDENŢĂ CONTABILĂ

9.1. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor din sistemul de evidenţă contabilă, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

9.2. Se utilizează tehnologii şi mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor şi constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informaţiilor din sistemul de evidenţă contabilă.

9.3. Se asigură testarea funcţionării corecte a componentelor de securitate a sistemului de evidenţă contabilă (automat – la pornirea sistemului, şi după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

9.4. Copiile de siguranţă: reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranţă a informaţiilor din sistemul de evidenţă contabilă şi soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a

copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENŢĂ CONTABILĂ

10.1. Persoanele care asigură exploatarea sistemului de evidenţă contabilă trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidenţă contabilă.

10.3. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din sistemul de evidenţă contabilă poartă răspundere pentru acţiunile neconforme comise intenţionat.

XI. DISPOZIŢII FINALE

11.1. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea Inspectoratului periodic, însă cel puţin o dată la 2 (doi) ani, precum şi la necesitate.

11.2. Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

11.3. Regulamentul este adus la cunoştinţă angajaţilor contra semnăturii.

11.4. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.

APROBAT
prin Ordinul Şefului IPM
nr. 14 din 01.02. 2023

L.Ş

REGULAMENTUL
privind protecţia datelor cu caracter personal în procesul evidenţei şi circulaţiei corespondenţei, atât la nivelul aparatului central al Inspectoratului pentru Protecţia Mediului, cât şi a subdiviziunilor teritoriale a acestuia

I. Dispoziţii generale

1. Regulamentul privind protecţia datelor cu caracter personal în procesul evidenţei şi circulaţiei corespondenţei Inspectoratului pentru Protecţia Mediului *(în continuare - Regulamentul)* este elaborat în conformitate cu prevederile Codului administrativ al Republicii Moldova, aprobat prin Legea nr.116/2018, Legii nr.71-XVI din 22 martie 2007 cu privire la registre, Legii nr.133/2011 privind protecţia datelor cu caracter personal, Instrucţiunilor privind ţinerea lucrărilor de secretariat referitoare la petiţiile persoanelor fizice şi juridice, adresate organelor de stat, întreprinderilor, instituţiilor şi organizaţiilor Republicii Moldova, aprobate prin Hotărîrea Guvernului nr.208/1995, Regulilor de întocmire a documentelor organizatorice şi de dispoziţie şi Instrucţiunii-tip cu privire la ţinerea lucrărilor de secretariat în organele administraţiei publice centrale de specialitate şi ale autoadministrării locale ale Republicii Moldova, aprobate prin Hotărîrea Guvernului nr.618/1993, Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123/2010.

2. Prezentul Regulament reglementează modalitatea ţinerii Registrului de evidenţă a corespondenţei al Inspectoratului pentru Protecţia Mediului şi subdiviziunile sale teritoriale *(în continuare - Inspectorat)*, protecţia datelor cu caracter personal, precum şi procedura de înregistrare, securizare, modificare şi radiere a datelor din acest Registru.

3. Noţiunile utilizate în prezentul Regulament au semnificaţia prevăzută de Legea cu privire la registre, Codului administrativ al Republicii Moldova, aprobat prin Legea nr.116/2018, Legea privind protecţia datelor cu caracter personal, Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

Astfel, în sensul prezentului Regulament se definesc următoarele noţiuni:

Petiţie – orice cerere, sesizare sau propunere adresată unei autorităţi publice de către o persoană fizică sau juridică;

Cerere – orice cerere prin intermediul căreia se solicită emiterea unui act administrativ individual sau efectuarea unei operaţiuni administrative;

Sesizare – orice sesizare prin intermediul căreia se informează autoritatea publică cu privire la o problemă de interes personal sau public;

Propunere – orice propune prin intermediul căreia se urmăreşte realizarea de către

autoritatea publică a unor acţiuni de interes public;

Registrul de evidenţă a corespondenţei – resursa informaţională specializată (totalitatea informaţiilor ţinute în formă automatizată şi manuală) care asigură evidenţa informaţiei sistematizate, principalul obiectiv al căruia constă în asigurarea evidenţei corespondenţei de intrare/ieşire a Inspectoratului;

Registrul electronic – sistem automatizat de evidenţă, bazat pe sisteme IT care asigură evidenţa, sistematizarea şi stocarea informaţiei referitor la corespondenţa de intrare/ieşire a Inspectoratului;

Registrator – angajatul Inspectoratului împuternicit cu atribuţiile de introducere, modificare, păstrare a informaţiei din Registru.

Furnizorul datelor - persoana fizică sau reprezentantul persoanei juridice de drept public sau privat, care prezintă registratorului date despre obiectul registrului în modul stabilit de lege sau acord.

4. Subiecţi ai raporturilor juridice apărute ca rezultat al instituirii, administrării şi ţinerii manuale a Registrului sunt:

a) Inspectorat, în calitate de proprietar şi deţinător al Registrului;

b) Persoanele împuternicite de ţinerea Registrului şi cele responsabile de efectuarea controlului intern al ultimului;

c) Persoanele fizice, ale căror date cu caracter personal vor fi stocate în Registru;

d) Persoanele interesate de a accesa şi vizualiza datele din Registru.

5. Angajaţii Inspectoratului poartă răspundere personală pentru îndeplinirea cerinţelor prezentului Regulament, asigurarea confidenţialităţii, securităţii şi păstrarea în stare corespunzătoare a informaţiei din Registru.

II. Formele Registrului şi condiţiile generale de ţinere a acestora

6. Registrul de evidenţă a corespondenţei *(în continuare - Registru)* a Inspectoratului reprezintă un sistem mixt ce utilizează atât evidenţa în formă electronică, cât şi în formă manuală.

7. În calitate de Registru electronic de evidenţă a corespondenţei, în cadrul Inspectoratului este utilizat sistemul informaţional „E-Management" *(în continuare - Sistem)*, care este instrumentul de bază în procesul de evidenţă a corespondenţei, pentru aparatul central şi subdiviziunile teritoriale ale Inspectoratului.

8. În vederea asigurării plenitudinii evidenţei actelor şi informaţiilor cu care se operează în activitatea Inspectoratului, se va asigura suplimentar, evidenţa fizică, pe bază de registre de hârtie a produselor activităţii administrative, inclusiv a corespondenţei de intrare şi ieşire a Inspectoratului.

9. Responsabil pentru derularea optimă a procesului de evidenţă a corespondenţei este Serviciul managementul documentelor a Inspectoratului *(în continuare - Serviciul)*, care va asigura gestionarea eficientă a sistemului şi coordonarea activităţii subdiviziunilor teritoriale sub aspectul utilizării acestuia.

10. Obiectul înregistrării în Sistem şi registrele de hârtie reprezintă informaţia referitor la persoanele care au depus înscrisuri în adresa Inspectoratului, subiectul şi obiectul adresării înaintate şi alte informaţii conţinute în acestea, inclusiv cele generate de activităţile administrative efectuate.

11. Registrul va fi ţinut în limba de stat.

12. Registratorul este obligat:

a) să introducă în Registru numai informaţie veridică, colectată de la adresant sau din alte surse neinterzise de lege;

b) să asigure evidenţa în ordine cronologică a fiecărei înscrieri în Registru;

c) să nu admită modificarea neîntemeiată a datelor introduse în Registru;

d) să efectueze înregistrările în Registru astfel, încât 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);

e) să asigure accesul la informaţia din Registru doar persoanelor care au dreptul de a primi informaţia respectivă, în conformitate cu legislaţia în vigoare;

f) să prevină accesul neautorizat la datele din Registru, utilizarea, difuzarea, modificarea sau nimicirea lor ilegală.

13. Datele din registru vor reflecta starea veridică şi actuală a informaţiei privind persoanele vizate în corespondenţa Inspectoratului.

14. Atât forma electronică cât şi cea manuală a Registrului va cuprinde în mod obligatoriu:

a) denumirea Registrului;

b) denumirea Inspectoratului ca proprietar, posesor şi deţinător al Registrului;

c) numele, prenumele şi funcţia persoanei responsabile de introducerea datelor în Registru şi a administratorului acestuia;

d) numele, prenumele şi funcţia persoanei care va exercita controlul asupra ţinerii Registrului;

e) numărul Registrului, termenele de ţinere şi păstrare a acestuia.

15. Datele cu caracter personal din Registru vor fi prelucrate în condiţiile stabilite de legislaţia privind protecţia datelor cu caracter personal. În acest sens, vor fi realizate măsuri de asigurare a gradului de exactitate a datelor registrului şi de protecţie a acestora contra distrugerii întâmplătoare sau neautorizate, modificării, dezvăluirii sau oricăror alte acţiuni ilegale la ţinerea registrului.

III. Condiţii generale privind introducerea informaţiei în Registru

16. Informaţia privind corespondenţa parvenită în adresa Inspectoratului va fi recepţionată şi înregistrată în aceiaşi zi de persoana responsabilă din cadrul Serviciului sau subdiviziunii teritoriale desemnate în acest sens în Sistem (document scanat), iar, versiunea de hârtie parvenită, se înregistrează în Registrul de hârtie al Inspectoratului sau subdiviziunii teritoriale.

17. La înregistrarea corespondenței, pe prima pagină se va aplica ştampilă de înregistrare în care se indică data primirii şi indicele de înregistrare. Indicele de înregistrare constă după caz, din numărul şi data de înregistrare a înscrisului.

18. După înregistrare, se va întocmi fişa de evidenţă şi control pentru adresările parvenite, introducându-se datele ce vizează petiţionarul, inclusiv, datele cu caracter personal (nume, prenume/denumirea p/j, adresa de domiciliu/adresa juridică, numărul de telefon/mail) precum şi rezoluţia conducerii Inspectoratului sau subdiviziunii teritoriale, termenul de soluţionare stabilit, datele despre starea executării şi semnătura executorului etc.

19. Modificările şi radierile făcute în Registru se efectuează în baza deciziei conducerii Inspectoratului, a subdiviziunii teritoriale şi cu semnătura registratorului în situaţia existenţei unui motiv întemeiat în acest sens.

20. Dacă furnizorul datelor registrului se adresează cu un demers argumentat privind rectificarea datelor eronate sau inexacte, registratorul va face, în modul stabilit, corectările necesare şi va informa despre aceasta furnizorul datelor.

21. Greşelile de ordin tehnic comise de către persoana împuternicită de ţinerea Registrului se rectifică de către aceasta. Corectarea greşelii se specifică într-o rubrică aparte, urmată de semnătura persoanei care a efectuat înscrierea.

22. Radierea obiectului din Registru se face prin inserarea unei note speciale (care trebuie să conţină semnăturile persoanei responsabile şi data radierii) şi nu reprezintă excluderea fizică a datelor despre obiect din Registru.

23. Nu se admit rectificări şi radieri ale înscrisurilor din Registru în alte condiţii decât cele stipulate în acest capitol.

IV. Condiţii generale privind păstrarea şi furnizarea informaţiei din Registru

24. Păstrarea Registrului este asigurată pînă la adoptarea deciziei conducerii Inspectoratului despre lichidarea Registrului, dar nu mai mult decât pe perioada stabilită de Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova.

25. Ţinerea Registrului este supusă controlului intern şi extern, în conformitate cu prevederile art.31 al Legii cu privire la registre.

26. În acest sens, persoana împuternicită de ţinerea şi păstrarea Registrului este obligată:

a) să prevină accesul nesancţionat la datele stocate în Registru;

b) să întreprindă acţiuni în vederea neadmiterii cazurilor de utilizare ilegală, dezvăluire ilegală a informaţiei conţinute în acesta, de modificare sau nimicire a acestor date.

27. Persoanele împuternicite de ţinerea şi controlul registrului sunt obligate să nu divulge informaţia la care au primit acces în legătură cu exercitarea atribuţiilor funcţionale, inclusiv după încetarea activităţii în cadrul Inspectoratului.

28. Registratorul este obligat să asigure accesul la informaţia din Registru pentru angajaţii autorizaţi ai Inspectoratului şi alte persoane, care au dreptul de a primi informaţia respectivă, în conformitate cu legislaţia în vigoare sau care demonstrează dreptul şi interesul legitim de a primi aceste informaţii, din momentul în care acestea vor fi disponibile, dar nu mai târziu de 5 zile lucrătoare de la data depunerii cererii.

29. Informaţia poate fi furnizată gratuit sau contra plată în conformitate cu Legea privind accesul la informaţie.

30. Extrasul din Registru trebuie să fie semnat de conducerea Inspectoratului sau subdiviziunii teritoriale, cu indicarea datei întocmirii/eliberării acestuia.

V. Condiţiile suplimentare privind gestionarea Registrului în forma manuală

31. Evidenţa corespondenţei în cadrul Inspectoratului sau subdiviziunii teritoriale este dusă prin intermediul mai multor Registre ţinute în formă manuală şi gestionate de persoane desemnate, cum ar fi:

a) „Registrul de intrare şi ieşire a petiţiilor adresate;

b) „Registrul de intrare/ieşire a corespondenţei" şi alte Registre instituite conform competenţei şi atribuţiilor Inspectoratului.

32. Registratorul, în cazul gestionării Registrului în formă manuală, este obligat:

a) să efectueze înscrierile citeţ şi clar. Prescurtările vor fi făcute astfel pentru a fi evitate diferite interpretări. Textul greşit se taie cu o linie, fiind posibilă citirea textului greşit înscris.

b) să nu înlocuiască neîntemeiat filele din cartea Registrului prin extragerea lor, încleierea unor noi file, etc;

c) să asigure, în cazul deteriorării cărţii, posibilitatea restabilirii imediate a datelor din registru fără a cauza daune informaţiei, ce se conţine în ea;

d) să asigure şnuruirea cărţilor pentru înregistrări (în caz că nu este o carte integrală) şi numerotarea filelor. Numărul de file se indică pe ultima pagină şi se autentifică (inclusiv conţinutul cărţii) prin aplicarea semnelor de control de către conducerea Inspectoratului sau subdiviziunii teritoriale: semnătură şi ştampilă.

33. Informaţia va fi introdusă în Registru în ordine cronologică, ţinându-se cont de necesitatea prezenţei menţiunilor privind:

a) numărul de ordine a menţiunii;

b) numărul şi data de intrare;

c) numele şi prenumele petiţionarului;

d) conţinutul succint al documentului;

e) numele şi prenumele executantului, termenul de executare şi rezoluţia conducerii Inspectoratului sau conducătorului subdiviziunii teritoriale;

f) rezultatul examinării: admisă/respinsă/oferite explicaţii de rigoare/acte de reacţionare adoptate de conducerea Inspectoratului sau subdiviziunii teritoriale.

34. Registrul în format de hârtie se păstrează de persoana responsabilă într-un safeu metalic şi va conţine un compartiment separat în care se vor consemna înregistrările de

audit a securității, prevăzute de pct.93 al Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

VI. Condiții suplimentare privind gestionarea Registrului în formă electronică

37. Ținerea în formă electronică a Registrului de evidență a corespondenței este realizat de Inspectorat prin intermediul sistemului informațional automatizat special constituit - Sistemul informatic „E-Management".

38. Introducerea, modificarea și păstrarea informației în acest Registru este asigurată de registratorul desemnat din cadrul Serviciului managementul documentelor pentru corespondența parvenită în cadrul Inspectoratului (aparatul central) sau din cadrul subdiviziunii teritoriale pentru corespondența parvenită în unitatea teritorială.

39. La înscrierea informației privind corespondența parvenită, în Registru se inserează și o listă de date despre obiect, inclusiv date cu privire la faptul înregistrării în compartimentele special destinate, și anume:

a) tipul adresării;

b) data și numărul de intrare;

c) termenul de rezolvare și data expirării;

d) numele, prenumele adresantului;

e) adresa de domiciliu, e-mail (în cazul existenței);

f) numărul de telefon fix/mobil;

g) conținutul succint al adresării;

h) rezoluția conducerii;

i) persoana responsabilă de control și executorul;

j) copia scanată, în format „.pdf" a adresării;

k) date privind executarea;

l) date privind posibila prelungire (termenul, numărul documentul prin care s-a efectuat prelungirea și informarea adresantului);

m) rezultatul examinării: admisă/respinsă/oferite explicații de rigoare/acte de reacționare adoptate.

n) copia scanată, în format „.pdf" a răspunsului.

VII. Măsurile de protecție a datelor cu caracter personal prelucrate în registrul de evidență a corespondenței

40. În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronic care conțin date preluate din Registrul de evidență a corespondenței, aceștia se păstrează în safeuri care se încuie.

41. La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.

42. Operatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.

43. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din Registrul de evidenţă a corespondenţei este blocat împotriva vizualizării de către persoane neautorizate.

44. Mijloacele de prelucrare a informaţiilor preluate din Registrul de evidenţă a corespondenţei sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

45. Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din Registrul de evidenţă a corespondenţei din/în perimetrul de securitate se înregistrează întru-n registru specializat.

46. Măsurile de protecţie a datelor cu caracter personal, prelucrate în Registrul de evidenţă a corespondenţei, se înfăptuiesc ţinând cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică şi externă.

47. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din Registrul de evidenţă a corespondenţei, care conţin date cu caracter personal, sunt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspândirea acestora.

Model: Atenţie! *Documentul conţine date cu caracter personal, iar prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr.133/2011 privind protecţia datelor cu caracter personal.*

48. Accesul în biroul unde este amplasat Registrul de evidenţă a corespondenţei este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi/sau cheia de la lacătul mecanic.

49. Biroul nu este lăsat niciodată fără supraveghere la ieşirea în exterior, uşa biroului se încuie cu lacătul.

50. Înainte de acordarea accesului fizic la Registrul de evidenţă a corespondenţei, se verifică competenţele de acces.

51. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în Registrul supus lichidării se transmit în arhivă, conform cerinţelor prevăzute în instrucţiunile cu privire la ţinerea lucrărilor de secretariat.

52. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat Registrul de evidenţă a corespondenţei, fiind integru din punct de vedere fizic, acesta zilnic, se inspectează sub aspectul integrităţii fizice.

53. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine.

54. Amplasarea Registrului de evidenţă a corespondenţei răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

55. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii Registrul de evidenţă a corespondenţei, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor

nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii, inclusiv posibilitatea deconectării oricărui component TI.

56. Computerele, unde este amplasat Registrul de evidenţă a corespondenţei, dispun de UPS-uri, care sunt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

57. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din Registrul de evidenţă a corespondenţei, sunt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaţionale.

58. Securitatea anti incendiară a registrului de evidenţă a corespondenţei: biroul unde este amplasat registrul de evidenţă a corespondenţei este dotat cu echipament anti incendiar şi corespunde cerinţelor şi normelor anti incendiare în vigoare.

59. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul Registrul de evidenţă a corespondenţei. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

VIII. Identificarea şi autentificarea utilizatorului Registrului de evidenţă a corespondenţei

60. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din Registrul de evidenţă a corespondenţei şi a proceselor executate în numele acestor utilizatori.

61. Toţi utilizatorii (inclusiv administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

62. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lângă cerinţele de păstrare a confidenţialităţii parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepţia cazului de asigurare a securităţii păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

63. Se efectuează modificarea parolelor de fiecare dată când sunt depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.

64. Întru asigurarea posibilităţii de stabilire a responsabilităţii fiecărui utilizator, sunt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. După trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.

65. Se asigură, pentru o perioadă de 1 */un/* an, păstrarea istoriilor anterioare ale parolelor în formă de cash a utilizatorilor şi prevenirea folosirii repetate a acestora.

66. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizaţii de acces primite în scopul comiterii unei fapte prejudiciabile, absenţă a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi autentificare se revocă sau se suspendă.

67. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în Registrul de evidenţă a corespondenţei, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în registrul de evidenţă a corespondenţei, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 */una/* lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informaţiile din Registrul de evidenţă a corespondenţei. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

68. În scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la Registrul de evidenţă a corespondenţei.

69. Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autorizează de persoanele responsabile.

70. Se impun limite în privinţa persoanelor care au dreptul:

71. să vizualizeze informaţiile stocate în Registrul de evidenţă a corespondenţei;

72. b) să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

73. Toţi angajaţii cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor cu caracter personal.

74. Orice activitate de dezvăluire a datelor cu caracter personal către terţi este documentată şi supusă unei analize riguroase în prealabil privind scopul şi temeiul legal a intenţiilor de dezvăluire a unui anumit volum de date cu caracter personal.

75. Orice încălcare a securităţii în ceea ce priveşte Registrul de evidenţă a corespondenţei este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

76. Înainte de acordarea accesului în sistem, utilizatorii sunt informaţi despre faptul că folosirea Registrului de evidenţă a corespondenţei este controlată şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia civilă, contravenţională şi penală.

IX. Auditul securităţii în sistemele de evidenţă a documentelor

77. Se organizează generarea înregistrărilor de audit a securității în Registrul de evidenţă a corespondenţei pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

78. 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.

79. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării informaţiilor din Registrul de evidenţă a corespondenţei, 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 al procesului;

c) ID-ul utilizatorului;

d) rezultatul tentativei de pornire – pozitivă sau negativă.

80. Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informaţiilor din Registrul de evidenţă a corespondenţei, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);

b) denumirea (identificatorul) aplicaţiei sau a 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.

81. Se efectuează 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.

82. Se efectuează înregistrarea ieşirii din Registrul de evidenţă a corespondenţei, 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, filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

85. Cazurile de deranjament al auditului securităţii în Registrul de evidenţă a corespondenţei sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sunt aduse la cunoştinţa persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

86. Rezultatele auditului securităţii în Registrul de evidenţă a corespondenţei (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.

87. Durata minimă a stocării rezultatelor auditului securităţii în Registrul de evidenţă a corespondenţei constituie 2 */doi/* ani, în scopul asigurării posibilităţii de folosire a 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.

X. Asigurarea integrităţii informaţiilor din Registrul de evidenţă a corespondenţei

88. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor din registrul de evidenţă a corespondenţei, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

89. Se utilizează tehnologii şi mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor şi constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informaţiilor din Registrul de evidenţă a corespondenţei.

90. Se asigură testarea funcţionării corecte a componentelor de securitate a Registrului de evidenţă a corespondenţei (automat – la pornirea sistemului, şi după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

91. Copiile de siguranţă: reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranţă a informaţiilor din Registrul de evidenţă a corespondenţei şi soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

XI. Gestionarea incidentelor de securitate a Registrului de evidenţă a corespondenţei

92. Persoanele care asigură exploatarea Registrului de evidenţă a corespondenţei trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

93. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în Registrul de evidenţă a corespondenţei.

94. În cazul producerii incidentelor de securitate persoanele responsabile vor întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, vor efectua analiza acestuia şi vor înlătura cauzele incidentului de securitate.

95. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din Registrul de evidenţă a corespondenţei poartă răspundere pentru acţiunile neconforme comise cu intenţie.

XII. Dispoziţii finale

96. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea Inspectoratului periodic, însă cel puţin o dată în 2 (doi) ani, precum şi la necesitate.

97. Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

98. Regulamentul este adus la cunoştinţa angajaţilor contra semnăturii.

99. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.