APROBAT
Prin Ordinul IPM
nr. 19 din 11.03.2021

L.Ş.

POLITICA DE SECURITATE

PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR INFORMAȚIONALE GESTIONATE DE INSPECTORATUL PENTRU PROTECȚIA MEDIULUI

CHIȘINĂU 2021

I. Preambul

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

II. Introducere

Inspectoratul pentru Protecția Mediului *(în continuare - Inspectorat)* are sediul înregistrat în mun. Chișinău, str. Cosmonauților, 9, Republica Moldova.

Politica de Securitate „Privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de Inspectoratul pentru Protecția Mediului" *(în continuare – Politica de Securitate)* este aprobată de către șeful Inspectoratului pentru Protecția Mediului, care acționează în baza legislației: Legea nr. 1515 din 16.06.1993 privind protecția mediului înconjurător și Hotărîrea Guvernului nr. 548 din 13.06.2018 cu privire la organizarea și funcționarea Inspectoratului pentru Protecția Mediului.

Prezenta Politică de securitate este aprobată, inclusiv, în vederea conformării Inspectoratului cu prevederile Hotărârii Guvernului Republicii Moldova nr.1123 din data de 14 decembrie 2010 "privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal" și Legii Republicii Moldova nr.133 din 08.07.2011 "privind protecția datelor cu caracter personal".

III. Noțiuni generale

În prezenta Politică de Securitate, sînt definite/utilizate următoarele noțiuni:

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

categorii speciale de date cu caracter personal – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancțiunile contravenționale;

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

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

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

control de securitate - acţiuni întreprinse de către Inspectoratul pentru Protecţia Mediului în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute;

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

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

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

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

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

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

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

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

protecţia informaţiei contra acţiunilor neintenţionate — ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum şi la pierderea, distrugerea acesteia

sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;

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

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

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

utilizator – persoana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;

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

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

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;

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

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

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

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

IV. Obiectivele Politicii de Securitate

Obiectivele principale ale Politicii de Securitate sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de Inspectorat, atît în cadrul prelucrării manuale, cît şi sistemelor şi proceselor de tehnologie informaţională.

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

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

Inspectoratul va proteja datele cu caracter personal atît a participanţilor la proces/vizitatori, cît şi a angajaţilor săi.

Reglementările prezentei Politici de Securitate reprezintă un standard minim pentru Inspectorat, inclusiv pentru toţi angajaţii acestuia.

Pornind de la această reglementare, toţi angajaţii Inspectoratului urmează să respecte strict prevederile Politicii de Securitate şi regulilor interne ale Inspectoratului privind protecţia datelor cu caracter personal şi sistemelor IT.

Prevederile Politicii de Securitate se aplică tuturor angajaţilor Inspectoratului care sunt implicaţi direct sau indirect în procesul de colectare, prelucrare şi păstrare a datelor cu caracter personal precum şi altor persoane fizice şi juridice *(petiţionari, candidaţii la funcţiile publice, agenţi economici, contravenienţi, studenţi care desfăşoară stagiul de practică etc.)*.

Politica de Securitate determină datele cu caracter personal ca fiind orice informaţie referitoare la angajaţii Inspectoratului şi la sistemul de salarizare al acestora, informaţiile obţinute în cadrul procedurilor contravenţionale, de control şi alte acţiuni desfăşurate conform competenţelor atribuite, cu excepţia datelor care potrivit prevederilor legale sunt publice.

V. Dispoziţii privind ierarhia şi responsabilitatea persoanei responsabile de Politica de securitate

Operatorul de date cu caracter personal reieşind din specificul activităţii, prin prezenta Politică de Securitate, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecţie la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidenţă gestionate.

Politica de Securitate a datelor cu caracter personal se va revizui cel puţin o dată în an ca rezultat al modificărilor sau reevaluării competenţelor entităţii, fiind pusă în sarcina conducătorilor, de a desemna persoana/ele care vor purcede nemijlocit la ajustarea prevederilor prezentului act.

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.

Responsabil de implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, va fi desemnată persoana care conform

fişei postului şi/sau ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

Persoana responsabilă desemnată, indiferent de funcţiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit conducătorului Inspectoratului sau persoanei care îndeplineşte interimatul funcţiei.

Persoana responsabilă de Politica de Securitate asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

Persoana responsabilă de Politica de Securitate personal va defini clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală, va asigura măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal, va elabora procedurile de clasificare a informaţiei care conţine date cu caracter personal astfel încît să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date, va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

VI. Mijloacele supuse principiilor de protecţie a datelor cu caracter personal

Protecţia datelor cu caracter personal în cadrul Inspectoratului *(în calitate de operator de date cu caracter personal)* este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal.

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

- suporturi magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;
- sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionări şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei;
- suporturi de hîrtie, registre, dosare, nomenclatoare, rapoarte etc..

VII. Măsurile de protecţie a datelor cu caracter personal sînt asigurate în scopul:

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

b) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;

c) neadmiterea dezvăluirii terţilor a informaţiei cu accesibilitate limitată;

d) eficientizarea resurselor informaţionale atît pe suport de hîrtie cît şi cel în format electronic.

VIII. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:

a) preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele,

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

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

d) preîntîmpinarea 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,

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

f) preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale.

IX. Procedurile organizatorice şi tehnice care urmează a fi respectate în cadrul Inspectoratului pentru Protecţia Mediului la prelucrarea datelor cu caracter personal

1. Măsurile generale de administrare a securităţii informaţionale

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

b) Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.

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

d) 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.

e) Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în scopul exercitării atribuţiilor de serviciu, sau, necesităţi logistice.

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

g) Este interzisă instalarea programelor de tip Shareware sau freeware, fară aprobarea administratorului sistemului informatic.

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

a) Accesul în sediile/oficiile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară, conform listei sau însemnelor corespunzătoare (legitimaţii, insigne, ecusoane, cartele de identificare).

b) Se asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces.

c) Perimetrul de securitate a Inspectoratului reprezintă perimetrul oficiilor în care se prelucrează/stochează date cu caracter personal.

d) Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sînt rezistenţi, intrările sunt echipate cu lacăte, semnalizare şi după caz, mecanisme automatizate de acces.

e) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

f) Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc membrii.

g) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

h) Accesul în perimetrul de securitate a clădirii Inspectoratului unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ţinînd cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 şi art. 30 ale Legii privind protecţia datelor cu caracter personal, precum şi pct. 26 din Cerinţe.

i) Folosirea tehnicii foto, video, audio, de telefonie sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii conform regulamentului aprobat în acest sens..

3. Identificarea şi autentificarea utilizatorilor

a) Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.

b) Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care conţine semnalmentele nivelului de accesibilitate al utilizatorului.

c) Pentru confirmarea ID-ului utilizatorului sînt utilizate parole sau alte soluţii disponibile.

d) În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date

cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă sau se suspendă.

4. Identificarea şi 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 perioadă îndelungată.

5. Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:

- identificarea univocă a fiecărui utilizator,
- verificarea autenticităţii fiecărui utilizator.

6. Utilizarea parolelor în procesul asigurării securităţii informaţionale

Sunt respectate regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:

- păstrarea confidenţialităţii parolelor,
- interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia,
- modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei,
- alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere,
- modificarea parolelor peste intervale de 3 luni,
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

7. 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.

8. Accesul de la distanţă

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

b) 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.

9. Limitarea folosirii tehnologiilor fără fir

a) Accesul fără fir la sistemele informaţionale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării şi controlului.

b) Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.

c) Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale Inspectoratului.

10. Securitatea electroenergetică

a) 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.

b) 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.

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

11. Controlul instalării şi scoaterii componentelor T.I.

a) 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.

b) Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.

12. Categoriile de date cu caracter personal prelucrate şi a operaţiunilor de prelucrare efectuate asupra acestora

a) Categoria obişnuită de date cu caracter personal cum ar fi: numele şi prenumele; sexul; data şi locul naşterii; cetăţenia; IDNP; imaginea; situaţia familială; situaţia militară; datele din certificatul de înmatriculare; situaţia economică şi financiară; datele privind bunurile deţinute; datele bancare; semnătura; datele din actele de stare civilă; codul personal de asigurării sociale (CPAS); codul asigurării medicale (CPAM); numărul de telefon/fax; numărul de telefon mobil; adresa (domiciliului/reşedinţei); adresa e-mail; profesia şi/sau locul de muncă; formarea profesională - diplome - studii;

b) Categoriile speciale de date cu caracter personal: obişnuinţele/preferinţele/comportamentul; sancţiuni administrative, măsurile procesuale de constrîngere sau sancţiunile contravenţionale, precum şi cele referitoare la condamnările penale.

c) Nu sunt înregistrate şi nu sunt prelucrate categoriile 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.

13. Inspectoratul prelucrează datele cu caracter personal în conformitate cu prevederile actelor normative din domeniu, în calitate de operator, prin intermediul subdiviziunilor sale, pentru derularea următoarelor activităţi:

a) Evidenţa şi managementul angajaţilor.

b) Evidenţa contabilă şi salarizare.

c) Achiziţii publice.

d) Evidenţa documentelor, consultaţiilor şi vizitatorilor.

e) Gestionarea informaţiilor privind persoanelor supuse controlului şi procedurii contravenţionale;

f) Asigurarea relaţiilor cu persoanele fizice/ juridice de drept priva sau public prin examinarea adresărilor, plângerilor etc..

g) Întocmirea dosarelor administrative.

h) Gestionarea litigiilor pendinte, întocmirea actelor procedurale şi depunerea lor în instanţa de judecată, reprezentarea intereselor Inspectoratului.

i) Organizarea/derularea evenimentelor.

14. Prelucrarea datelor cu caracter personal include următoarele operaţiuni:

a) colectarea datelor conform atribuţiilor funcţionale;

b) înregistrarea în registre conform domeniilor de aplicare;

c) organizarea procesului de lucru cu datele şi asigurarea confidenţialităţii acestora;

d) stocarea datelor;

e) păstrarea şi arhivarea conform legislaţiei în vigoare.

15. Dezvăluirea datelor cu caracter personal

a) Dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată integritatea şi nedivulgarea datelor cu caracter personal. În cazul în care reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere *(expediere poştală cu aviz recomandat, înmînarea personală, etc.)*.

b) 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.)* sînt interzise.

c) Dezvăluirea datelor cu caracter personal prin transmiterea acestora pe suport de hîrtie se efectuează cu respectarea prevederilor legale privind confidenţialitatea datelor cu caracter personal şi doar în cazurile prevăzute de actele normative.

d) Sînt interzise operaţiunile de dezvăluire a datelor cu caracter personal între Inspectorat şi alte entităţi care sunt amplasate geografic în stînga 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 ţine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecţia datelor cu caracter personal.

e) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie şi/sau suport digital, peste hotarele Republicii Moldova, se efectuează cu respectarea actelor normative corespunzătoare.

f) Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecţia datelor cu caracter personal, în special în cazurile cînd tratatul internaţional în baza căruia se efectuează

transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal.

g) Volumul şi categoriile datelor cu caracter personal colectate în scopul ținerii evidenței contabile, a personalului, corespondenței, procedurii administrative, de control şi contravenționale etc. este limitat la strictul necesar pentru realizarea scopurilor declarate.

h) Acces la sistemele informaționale gestionate în cadrul Inspectoratului, din partea Procuraturii Generale *(după caz procuraturile teritoriale/specializate)*, Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi art. 212 Cod de procedură penală.

Se explică că în conformitate cu prevederile art.157 Cod de procedură penală, documentele în orice formă *(scrisă, audio, video, electronică etc.)* care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adeverite circumstanțe care au importanță pentru cauză, *(inclusiv informația stocată în auditul sistemelor informaționale şi de evidență)*, pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate şi răspîndite fără necesitate informație oficială cu accesibilitate limitată.

Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată *(inclusiv operatorii de date cu caracter personal)* au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date.

Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

Urmează a ține cont de faptul că în conformitate cu prevederile art.8 al Legii privind accesul la informație, datele cu caracter personal fac parte din categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoştință cu datele cu caracter personal al clientului, aceştia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 şi 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 74^1 Cod contravențional.

16. Drepturile subiecților de date cu caracter personal

a) În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecția datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informații, exceptînd cazul în care el deține deja informațiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator *(denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidență al operatorilor de date cu caracter personal);*

- privind scopul concret al prelucrării datelor cu caracter personal colectate;
- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existența drepturilor la informare și de acces la datele colectate; de intervenție asupra datelor *(în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora)* și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.

b) Subiecților de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum și 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 alți subiecți, conținute în fișele personale *(alte materiale),* cu excepția cazurilor în care solicitanții își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.

c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal *(sau entitățile ce asigură mentenanța sistemului și sau prestează servicii externalizare ale operatorului)* tuturor persoanelor supuse prelucrării.

d) În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse legale *(acte de identitate, de stare civilă, resurse informaționale principale de stat etc.),* modificarea urmînd a fi efectuată în toate sistemele informaționale și de evidență gestionate.

17. Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate

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

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

c) Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul Inspectoratului.

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

18. Auditul sistemelor informaţionale gestionate

a) 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.

b) 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, o 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.

c) Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) 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.

d) 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.

19. Asigurarea protecţiei contra programelor dăunătoare (virusilor)

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

20. Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

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

21. Gestionarea incidentelor de securitate

a) Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

b) Personalul Inspectoratului informează neîntîrziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.

c) Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor și restabilirea securității.

d) Pînă la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Autoritatea națională pentru protecția datelor cu caracter personal despre incidentele de securitate constatate.

22. Marcarea documentelor

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

Model: Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr. 000000X-00X, înregistrat în Registrul de evidență al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal

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

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, semnatari a anexei nr. 2, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 74^1 Cod contravențional) și penală (art. art. 177, 178, 180 Cod penal).

Anexa nr. 2
la Politica de Securitate privind protecţia datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale gestionate de inspectoratul pentru protecţia mediului

Consimţământ

la prelucrarea datelor cu caracter personal în cadrul Inspectoratului pentru Protecţia Mediului

Sistemul de evidenţă _____

Subsemnatul _____

Adresa _____

B.I seria _____nr. _____ din _____ of. _____ ,

IDNP /__/__/__/__/__/__/__/__/__/__/__/__/__/

în calitate de: _____

am luat cunoştinţă cu faptul că îmi pot exercita toate drepturile prevăzute de *Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal,* sunt de acord cu prelucrarea următoarelor date cu caracter personal : **numele, prenumele, patronimicul, sexul, data şi locul naşterii, semnătura, date din actele de stare civilă.** CP AM, **telefon mobil, e-mail, profesie, formare profesională- diplome-studii, situaţie familiară, situaţie economică sau financiară, imagine, datele membrilor de familie, cetăţenia, sancţiuni disciplinare,** CPAS, **telefon/fax, adresa domiciliului/reşedinţei, loc de muncă,** IDNP, **situaţie militară, date privind bunurile deţinute, obişnuinţe/preferinţe/comportament, caracteristici fizice,** în scopul _____ şi sunt de acord ca datele prezentate sa fie folosite în scopul propus.

semnătura **data**

Inspectoratul pentru Protecţia Mediului se obligă să utilizeze datele numai pentru destinaţia stabilită şi să asigure protecţia şi confidenţialitatea acestora conform Legii nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal şi a Politicii de securitate a datelor cu caracter personal în cadrul Inspectoratului pentru Protecţia Mediului aprobată prin Ordin.

Anexa nr. 1
la Politica de Securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de inspectoratul pentru protecția mediului

REGULAMENTUL
privind supravegherea prin mijloace video în cadrul Inspectoratului pentru Protecția Mediului

1. Dispoziții generale

În contextul actual securitatea obiectivelor nu poate fi asigurată fără o supraveghere video eficientă, care să permită, atît monitorizarea în timp real a evenimentelor și persoanelor suspecte, cît și înregistrarea imaginilor video.

Totodată utilizarea unui astfel de sistem include anumite responsabilități și garanții din partea proprietarului de sistem, referitor la prelucrarea și protecția datelor cu caracter personal ce se înregistrează în sistem, atribuții și reglementări descrise în legea nr. 133 din 18.07.2011 privind protecția datelor cu caracter personal.

Din acest motiv este necesară stabilirea unui Regulament de securitate privind supravegherea prin mijloace video și prelucrarea datelor cu caracter personal preluate și înregistrate în sistemul de monitorizare prin înregistrare video.

2. Regulamentul privind supravegherea prin mijloace video în cadrul Inspectoratului pentru Protecția Mediului *(în continuare - Regulament)* are drept scop:

1) Stabilirea unui set unitar de reguli care reglementează implementarea și utilizarea sistemului de supraveghere video, în scopul asigurării securității persoanelor și bunurilor, pazei și protecției bunurilor, imobilelor, valorilor și a materialelor cu regim special, respectînd în același timp obligațiile ce revin inspectoratului pentru Protecția Mediului *(în continuare - Inspectorat)*, în calitate de operator de date, conform Legii nr. 133 din 18.07.2011 și măsurile de securitate adoptate pentru protecția datelor cu caracter personal, protejarea vieții private, a intereselor legitime și garantarea drepturilor fundamentale ale persoanelor vizate.

2) Stabilirea responsabilităților privind administrarea și exploatarea sistemului de supraveghere prin mijloace video, precum și cele privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.

3) Scopul utilizării sistemului video este de a asigura buna administrare și funcționare a entității, în special în vederea controlului de securitate și pază. De asemenea, sistemul video este necesar pentru a sprijini politicile de securitate instituite de actele normative care reglementează protecția datelor cu caracter personal și contribuie la îndeplinirea atribuțiilor structurii de securitate.

4) Prezentul Regulamentul descrie măsurile care necesită a fi luate de Inspectorat pentru a proteja datele cu caracter personal care sînt prelucrate prin metoda supravegherii video, vieții private și alte drepturi fundamentale și interese legitime ale subiecților.

3. Zonele supravegheate

1) Camerele de supraveghere video sînt amplasate în locuri vizibile. Orice utilizare ascunsă a acestora este strict interzisă, cu excepția cazurilor expres reglementate de legislație.

2) Camerele de supraveghere video sînt amplasate conform anexei nr. 1 al prezentului Regulament.

3) Nu sînt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum birourile de serviciu și toaletele.

4. Datele cu caracter personal colectate prin intermediul sistemului de supraveghere video

1) Sistemul de supraveghere video este dotat cu detector de mișcare. Toate camerele funcționează în regim 24/24 ore și sînt fixate.

2) La darea în exploatare a sistemului de supraveghere video, persoana împuternicită v-a primi instructajul referitor la setările sistemului de monitorizare video, respectarea regimului de confidențialitate și dreptul de acces la informația prelucrată în sistemul de evidență.

5. Limitarea scopului

1) Sistemul de supraveghere video va fi utilizat numai în scopul în care este notificat, fără a se urmări în special obținerea unor informații pentru anchetele interne sau procedurile disciplinare, cu excepția situațiilor în care se produce un incident de securitate sau se observă un comportament infracțional (în circumstanțe excepționale imaginile pot fi transmise organelor competente în cadrul unor investigații disciplinare sau penale).

2) În vederea protejării vieții private a altor subiecți decît cei vizați nemijlocit, sistemul video este dotat cu mecanisme care prevăd estomparea imaginii (în caz de necesitate) pentru a face ca întreaga imagine sau o parte a ei, după caz, să fie anonimizată.

3) Persoana responsabilă va gestiona accesul la sistemul de supraveghere video numai cu acordul scris al conducerii Inspectoratului.

6. Categorii speciale de date cu caracter personal

Sistemul de monitorizare video al Inspectoratului nu are ca scop captarea (spre exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (spre exemplu indexare, creare de profiluri) care constituie categoria specială de date cu caracter personal.

7. Accesul la datele cu caracter personal și dezvăluirea acestora

1) Accesul la imaginile video înregistrate în timp real este limitat la un număr redus de angajați ai Inspectoratului, care pot fi identificați individual, în conformitate cu lista aprobată de către conducerea entității.

2) Accesul la imaginile video şi/ sau la arhiva în care sînt stocate imaginile înregistrate este permis numai persoanei responsabile în conformitate cu Politica de securitate a Inspectoratului şi numai cu acordul scris al conducerii.

3) Vizualizarea şi/sau efectuarea copiilor din fişierele temporare în care sînt stocate imaginile video, este permis numai cu acordul scris al conducerii Inspectoratului.

4) În cazul solicitării de către organele de drept ale Republicii Moldova, care își exercită atribuțiile conform legii, a unor copii din fişierele temporare în care sînt stocate imaginile video, este permis numai cu acordul scris al conducerii Inspectoratului.

8. Protecția sistemului informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video

În vederea securizării sistemului informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video, se aplică următoarele măsuri tehnice şi organizatorice:

a) sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video se păstrează în camera special amenajată;

b) responsabilul de protecție a datelor cu caracter personal şi responsabilii de securitate din cadrul entității vor fi consultați înainte de achiziționarea sau instalarea oricărui nou sistem de supraveghere.

c) toate sistemele trebuie să corespundă cerințelor de securitate descrise în legislație (HG nr. 1123 privind aprobarea cerințelor față de asigurarea securității datelor cu caracter personal).

d) accesul fizic la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video are numai persoana responsabilă desemnată şi conducerea Inspectoratului;

e) accesul la înregistrările video prelucrate este restricționat prin introducerea unui şir de parole;

f) în cazul deconectării energiei electrice, sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu sursă autonomă de alimentare cu energie electrică (UPS);

g) sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu firewall care asigură protecția în rețea;

h) Echipamentele sînt astfel instalate încît să se afle sub supraveghere doar acele spații identificate în analiza de risc ca având nevoie de protecție suplimentară.

i) Utilizatorii sistemului de supraveghere video sunt instruiți să nu monitorizeze astfel de zone.

j) Inspectoratul actualizează în permanență listă persoanelor care au acces la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video, care descrie în detaliu drepturile de acces ale acestora.

9. Control Acces

1) Imaginile captate de sistemul de supraveghere video sînt vizualizate în timp real pe monitorul/rele amplasate de regulă în camera de control acces, care reprezintă o încăpere securizată, iar monitoarele nu pot fi văzute din exterior, însă, monitorul/rele vizate pot fi amplasate şi în alte încăperi, unde accesul este restricţionat.

2) Camera de control acces este amplasată în sediul central al entităţii, după caz, poate fi amplasată şi în alte locaţii stabilite.

3) Accesul neautorizat în Camera de control este interzis. Accesul este strict limitat la angajaţii autorizaţi: personalul cu funcţii de asigurare al securităţii fizice şi control acces, administratorul de sistem, responsabilii cu securitatea informaţiei şi conducerea entităţii.

4) De la caz la caz, se poate acorda accesul în Camera de control şi altor persoane, în afara celor menţionate mai sus, doar pe bază de autorizare din partea responsabilului de securitate din cadrul entităţii. Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video, accesul acestora fiind permis strict pentru executarea lucrărilor menţionate în autorizarea din partea responsabilului de securitate din cadrul entităţii.

10. Pentru a proteja securitatea sistemului video şi pentru a spori gradul de protecţie a vieţii private, au fost introduse următoarele măsuri tehnice şi organizatorice:

a) limitarea timpului de stocare a materialului filmat, în conformitate cu cerinţele de securitate şi legislaţia în vigoare privind conservarea datelor.

b) mediile de stocare (serverele pe care se stochează imaginile înregistrate) se află în spaţii securizate şi protejate de măsuri de securitate fizică.

c) toţi utilizatorii cu drept de acces la sistemul de supraveghere video au semnat acorduri de confidenţialitate, prin care se obligă să respecte prevederile legale în domeniu.

d) utilizatorilor se acordă dreptul de acces doar pentru acele resurse care sînt strict necesare pentru îndeplinirea atribuţiilor de serviciu.

e) doar administratorii de sistem numiţi în acest sens de către operator, şi responsabilul de securitate, au dreptul de a accesa fişierele înregistrate în sistem, la cererea conducerii unităţii.

11. Drepturi de acces

1) Accesul la imaginile stocate şi/sau la arhitectura tehnică a sistemului de supraveghere video este limitat la un număr redus de persoane şi este determinat prin atribuţiile specificate în fişa postului, în care este indicat în ce scop şi ce tip de acces este acordat.

2) Inspectoratul impune limite stricte în privinţa persoanelor care au dreptul:

a) să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile responsabililor de securitate şi agenţilor de pază desemnaţi să desfăşoare activitatea de supraveghere;

b) să vizioneze înregistrarea materialului filmat: vizionarea imaginilor înregistrate se va face în cazuri justificate, cum ar fi cazurile prevăzute expres de lege şi incidentele de securitate, de către persoanele special desemnate;

c) să copieze, să descarce, să şteargă sau să modifice orice material filmat de sistemul de supraveghere video.

3) Instructaj

a) Toţi membrii personalului cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor cu privire la toate aspectele funcţionale, operaţionale şi administrative ale acestei activităţi.

b) Această procedură va fi integrată în programul de instruire şi îndrumare, pentru toţi utilizatorii cu drept de acces şi atribuţii în operarea sistemului de supraveghere video.

c) Imediat după instructaj, fiecare participant cu drept de acces la sistemul de supraveghere video semnează un acord de confidenţialitate.

12. Dezvăluirea datelor cu caracter personal

1) Orice activitate de dezvăluire a datelor personale către terţi va fi documentată şi supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, şi pe de altă parte compatibilitatea dintre scopul în care se face comunicarea şi scopul în care aceste date au fost colectate iniţial pentru prelucrare.

2) Orice situaţie de dezvăluire va fi consemnată de administratorul sistemului într-un Registru de evidenţă a cazurilor de dezvăluire.

3) Inspectoratul are obligația punerii la dispoziția organelor judiciare, la solicitarea scrisă a acestora, înregistrările video în care este surprinsă săvîrşirea unor fapte de natură contravențională/penală.

4) Sistemul de supraveghere video nu este utilizat pentru verificarea prezenței la program sau evaluarea performanței la locul de muncă.

5) În cazuri excepționale, dar cu respectarea garanțiilor descrise mai sus, se poate acorda acces altor servicii din cadrul entității (Protecție Antiincendiară, Resurse Umane, Riscuri), în cadrul unei anchete disciplinare, de accidentare sau de securitate, cu condiția ca informațiile să ajute la investigarea unei infracțiuni, accident de muncă sau a unei abateri disciplinare de natură să prejudicieze drepturile şi libertățile unei persoane fizice sau juridice.

13. Durata păstrării înregistrărilor video

1) Durata păstrării înregistrărilor video este de 30 zile calendaristice, după care acestea se nimicesc automat în ordinea în care au fost înregistrate.

2) În cazul producerii unui incident de securitate, durata de păstrare a înregistrărilor video poate depăşi limitele admisibile de program, în funcție de timpul necesar investigării suplimentare a incidentului de securitate.

14. Informarea publicului referitor la supravegherea video

1) Informarea publicului referitor la supravegherea video din cadrul Inspectoratului se efectuează prin pictograme.

2) Inspectoratul garantează că asigură respectarea drepturilor ce revin persoanelor vizate, în conformitate cu legislația Republicii Moldova. Toate persoanele implicate în activitatea de supraveghere video şi cele responsabile de administrarea imaginilor filmate, vor respecta procedurile şi regulamentele de acces la date cu caracter personal ale entității.

15. Informarea persoanelor vizate şi limitele de acces în locațiile Inspectoratului

1) Informarea primară a persoanelor vizate se realizează în mod clar şi permanent, prin intermediul unui semn adecvat, cu vizibilitate suficientă şi localizat în zona supravegheată, astfel încît să semnaleze existența camerelor de supraveghere, dar şi pentru a comunica informațiile esențiale privind prelucrarea datelor cu caracter personal.

2) Persoanele vizate sunt atenționate asupra existenței sistemului de supraveghere video şi a proprietarului prin note de informare corespunzătoare, care cuprind scopul prelucrării şi identifică Inspectoratul ca operator al datelor colectate prin intermediul supravegherii video.

3) Accesul persoanelor în locațiile Inspectoratului se permite doar cu însoțirea angajatului Inspectoratului care soluționează problema legată de persoana respectivă.

4) Accesul în locațiile Inspectoratului a persoanelor terțe cu dispozitive de înregistrare video-audio este restricționat şi se permite doar cu acordul conducerii Inspectoratului.

5) Inspectoratul informează persoanele terțe despre necesitatea depozitării temporare a mijloacelor de înregistrare audio-video, inclusiv, telefoane mobile şi gadgeturi într-un loc special amenajat de Inspectorat, pentru perioada aflării acestora în locațiile Inspectoratului.

6) Inspectoratul are dreptul de a limita accesul în locațiile Inspectoratului persoanelor care nu se conformează pct. 15. subpct.4) şi 5) a prezentului Regulament.

16. Exercitarea drepturilor de acces, intervenție şi opoziție

1) Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc, deținute de Inspectorat, de a solicita intervenția (ştergere/actualizare/rectificare/anonimizare) sau de a se opune prelucrărilor, conform legii.

2) Orice cerere de a accesa, rectifica, bloca şi/sau şterge date cu caracter personal ca urmare a utilizării camerelor video ar trebui să fie adresată direct conducerii Inspectoratului.

3) În cazul în care persoana vizată are alte întrebări privind prelucrarea de către Inspectorat a datelor personale care o privesc, se poate adresa conducerii Inspectoratului.

4) Răspunsul la solicitarea de acces, intervenție sau opoziție se dă în termen de 15 zile calendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amînare a răspunsului, de asemenea i se va comunica şi procedura care va urma pentru soluționarea cererii.

5) Dacă există solicitarea expresă a persoanei vizate, se poate acorda dreptul de a vizualiza imaginile înregistrate care o privesc sau i se poate trimite o copie a acestora. Imaginile furnizate vor fi

clare, în măsura posibilității, cu condiția de a nu prejudicia drepturile terților (persoana vizată va putea vizualiza doar propria imagine, imaginile altor persoanelor care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoașterea/identificarea lor). În cazul unei asemenea solicitări, persoana vizată este obligată:

a) să se identifice dincolo de orice suspiciune (să prezinte actul de identitate cînd participă la vizionare), să menționeze data, ora, locația și împrejurările în care a fost înregistrată de camerele de supraveghere.

b) De asemenea, persoana vizată va prezenta și o fotografie recentă astfel încît utilizatorii desemnați să o poată identifica mai ușor în imaginile filmate.

c) Persoana va putea vizualiza doar propria imagine, imaginile persoanelor care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoașterea/identificarea lor.

6) Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune și în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu dacă în imagini apar și alte persoane și nu există posibilitatea de a obține consimțământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

17. Auditul securității sistemului de monitorizare video

1) Auditul securității sistemului de monitorizare video menține înscrieri de sistem despre evenimentele produse în activitatea sistemului sau a aplicației, precum și despre activitatea utilizatorului.

2) În conjuncție cu instrumentele și procedurile respective, auditul securității sistemului de monitorizare video permite de a promova mijloace de ajutor pentru a atinge obiective de securitate: evidența acțiunilor utilizatorului, definirea și stabilirea responsabilității individuale, reconstrucția evenimentelor, detectarea intrușilor și problemelor de identificare a evenimentelor.

3) Auditul securității sistemului de monitorizare video este menit să acorde suport la:

a) stabilirea consecutivității acțiunilor utilizatorului sau proceselor;

b) stabilirea cînd, cine sau ce a stopat funcționarea normală a sistemului;

c) soluționarea problemei de detectare a intrușilor;

d) detectarea problemelor de funcționare a sistemului informatic în regim On-Line.

Anexa la
Regulamentul
privind supravegherea prin mijloace video
în cadrul Inspectoratului pentru Protecția Mediului

Lista cu locațiile pentru amplasarea camerelor de supraveghere în cadrul Inspectoratului pentru Protecția Mediului

I. Locațiile şi spaţiile de acces, destinate publicului din holul clădirii situat la et. 5, mun. Chişinău, str. Constantin Tănase, 9, unde se află sediul Inspectoratului;
1. Începutul holului (ambele părți) – cîte un dispozitiv video;
2. Pe segmentul holului – 6 dispozitive video;
3. Anticamera conducerii Inspectoratului;
4. Anticamera Inspecției pentru Protecția Mediului Chişinău - 1 dispozitiv video, cu sediul pe str. V Alecsandri, 1, mun. Chişinău.
5. Locațiile şi spațiile de acces al Inspecțiilor pentru Protecția Mediului teritoriale ale inspectoratului.