Anexă
la Hotărîrea Consiliului INJ
nr.2/2 din 22.02.2013

REGULAMENT
privind protecţia datelor cu caracter personal
ale salariaţilor din cadrul Institutului Naţional al Justiţiei

Sumar:

I. DISPOZIŢII GENERALE PRIVIND DATELE CU CARACTER PERSONAL

1.1. Prezentul Regulament dezvoltă şi concretizează reglementările legale referitoare la modul, condiţiile şi procedurile de protecţie a datelor cu caracter personal ale salariaţilor din cadrul Institutului Naţional al Justiţiei şi este emis în calitate de act normativ la nivel de instituţie în conformitate cu prevederile art.10 alin.(1) lit.e) din Codul muncii al Republicii Moldova.

1.2. Ca temei pentru elaborarea prezentului Regulament au servit următoarele acte normative: art.91 – 94 din Codul muncii al Republicii Moldova, Legea cu privire la protecţia datelor cu caracter personal nr.133 din 8 iulie 2011 şi Hotărîrea Guvernului privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal nr.1123 din 14.12.2010.

1.3. Prezentele dispoziţii, definesc următoarele noţiuni:

date cu caracter personal – orice informaţie referitoare la o persoană fizică, care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

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

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

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

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;

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

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

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

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;

tehnologie informaţională ((TI) eng. - informational technologic) – 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;

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.

1.4. În componenţa datelor cu caracter personal se includ informaţiile conţinute în: buletinul de identitate sau un alt act de identitate, carnetul de muncă, documentele de evidenţă militară, certificatul medical, diploma de studii. La fel, pot fi raportate la categoria datelor cu caracter personal şi datele autobiografice, informaţiile despre salariu ş.a.

II. MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL ŞI MECANISMELE DE PUNERE ÎN APLICARE A ACESTORA

2.1. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemul informaţional de date cu caracter personal se înfăptuiesc ţinîndu-se cont de necesitatea asigurării confidenţialităţii acestor măsuri, prin protecţia datelor personale în formă manuală, electronică şi externă.

2.1.1. Registrele în formă manuală - a angajaţilor, formatorilor şi audienţilor INJ - se păstrează în Secţia resurse umane şi documentare, în safeul Secţiei.

2.1.2. Registrele în formă electronică - a angajaţilor, formatorilor şi audienţilor INJ - se păstrează în contabilitate, în programul 1C, unde are acces o singură persoană – contabilul şef, prin care intră cu parolă în mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a Institutului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere.

Modificarea parolelor se efectuaează peste intervale de maximum 3 luni şi accesul fizic al altor persoane este strict interzis.

2.1.3. Protecţia externă a datelor personale ale salariatului se realizează prin: serviciul de pază, mijloace de signalizaţie sau alarmă antiincendiară.

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

2.3. Protecţia datelor cu caracter personal în sistemul informaţional este asigurată în scopul:
   a) preîntîmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
   b) preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;
   c) respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;
   d) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;
   e) păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.

2.4. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:
   a) preîntîmpinarea 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 angajaţi ai deţinătorului de date cu caracter personal, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program.

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

2.6. Mecanismul de punere în aplicare a măsurilor de protecţie este asigurat prin separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a

sistemelor informaţionale, prin izolarea funcţiilor de securitate de funcţiile care nu se atribuie la securitatea acestui sistem şi posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităţilor, a folosirii resurselor informaţionale în care sînt prelucrate date cu caracter personal.

2.7. Se efectuează monitorizarea permanentă şi controlul comunicaţiilor la perimetrul exterior al sistemelor informaţionale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaţionale.

2.8. Este asigurată imposibilitatea accesului din exterior a utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal, totodată asigurîndu-se integritatea şi confidenţialitatea datelor cu caracter personal transmise prin utilizarea mijloacelor de protecţie criptografică a informaţiei şi semnătura digitală.

III. SECURITATEA ŞI PROTECŢIA SISTEMULUI INFORMAŢIONAL ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

3.1. Prezentul Regulament se revizuieşte cel puţin o dată în an, ca rezultat al modificărilor sau reevaluării componentelor acestuia şi aprobat la cel mai înalt organ suprem de conducere al instituţiei – Consiliul INJ.

3.2. Directorul executiv numeşte prin ordin (Anexa 1) o persoană responsabilă de elaborarea, implementarea şi monitorizarea respectării prevederilor Regulamentului privind protecţia datelor cu caracter personal care vizează salariaţii din cadrul INJ, subordonată nemijlocit directorului instituţiei, care nu va avea alte responsabilităţi incompatibile cu sarcinile funcţiei de implementare a politicii.

3.3. Persoana responsabilă de politica de securitate a datelor cu caracter personal va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceastea nu operează în afara cadrului acestei politici, totodată va avea diferite 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.

3.4. Accesul în sediile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară- Directorul executiv, Directorul executiv adjunct, contabilul şef şi şeful Serviciului resurse umane şi documentare - şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare -insigne, ecusoane, cartele de identificare, cartele cu microprocesoare.

3.5. Se efectuează administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces şi competenţele de acces. Acordarea accesului fizic la sistemele informaţionale de date cu caracter personal se face prin registrele de monitorizare, care se păstrează minimum un an, la expirarea căruia acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

3.6. Perimetrul de securitate al clădirii sau încăperii în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal se determină concret, clar şi trebuie să fie integru din punct de vedere fizic. Pereţii exteriori ai încăperilor trebuie să fie rezistenţi, intrările

echipate cu lacăte, mijloace de control al accesului, semnalizare etc. În cazul amplasării încăperilor la parter şi/sau la ultimul etaj al clădirii, precum şi în cazul existenţei balcoanelor, scărilor antiincendiare, la ferestrele încăperilor respective se instalează gratii. Computerele, serverele, alte terminale de acces trebuie amplasate în locuri cu acces limitat pentru persoane străine. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii. Agendele şi/sau cărţile de telefoane în care se conţin indicii despre locul amplasării mijloacelor de prelucrare a datelor cu caracter personal nu vor fi accesibile persoanelor străine.

3.7. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal trebuie să răspundă necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii deţinătorului de date cu caracter personal. Purtătorii de informaţii şi mijloacele de prelucrare a datelor cu caracter personal scoase din încăperile aflate în perimetrul de securitate nu trebuie lăsate fără supraveghere în locuri publice.

3.8. Se asigură securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, trebuie asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI. Trebuie prevăzute surse autonome de alimentare cu energie electrică de scurtă durată, care sînt folosite pentru terminarea corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică. Cablurile de tensiune trebuie separate de cele comunicaţionale pentru a exclude bruiajul.

3.9. Deţinătorii de date cu caracter personal efectuează controale, nu mai rar decît o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea. Se prevăd mijloace de asigurare a securităţii antiincendiare a sediilor/oficiilor/birourilor unde sînt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal. Se exercită controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal.

3.10. 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. 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.

3.11. Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru. Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere. Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii deţinătorului de date cu caracter personal. Scoaterea şi introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează.

IV. IDENTIFICAREA, AUTENTIFICAREA ŞI ADMINISTRAREA ACCESULUI UTILIZATORULUI ÎN SISTEMUL INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

4.1. Se implementează mecanisme de înregistrare şi evidenţă a persoanelor care au acces sau participă la operaţiunile de prelucrare a datelor cu caracter personal şi care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

4.2. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.

4.3. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă sau se suspendă de către deţinătorul de date cu caracter personal.

4.4. Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Sînt folosite mijloace automatizate de suport în scopul administrării conturilor de acces. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp (pentru fiecare tip de cont de acces în parte). Sînt dezactivate automat, după o perioadă de maximum trei luni, conturile de acces ale utilizatorilor neactivi, care prelucrează date cu caracter personal. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

4.5. Este autorizat accesul la sistemele informaţionale de date cu caracter personal în conformitate cu politica de administrare a accesului stabilită de deţinătorul de date cu caracter personal. Accesul la funcţiile de securitate ale sistemului informaţional de date cu caracter personal şi la datele acestora este acordat doar persoanelor responsabile indicate expres în politica de securitate a deţinătorului de date cu caracter personal. Drepturile de acces ale utilizatorilor la sistemul informaţional de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni) şi după oricare schimbare de statut al utilizatorului.

4.6. Se autorizează de către deţinătorii de date cu caracter personal realizarea fluxurilor informaţionale în procesul transmiterii acestora în interiorul şi în afara sistemului informaţional de date cu caracter personal. Accesul fără fir la sistemul informaţional de date cu caracter personal este documentat, supus monitorizării şi controlului şi este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei. Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale deţinătorului de date cu caracter personal.

V. AUDITUL SECURITĂŢII ÎN SISTEMELE INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

5.1. Deţinătorii de date cu caracter personal organizează generarea înregistrărilor de audit a securităţii în sistemul informaţional de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

5.2. Înregistrările de audit a securităţii registrelor ţinute manual în care sînt prelucrate date cu caracter personal, trebuie să conţină:
a) numele şi prenumele utilizatorului;
b) numele fişei accesate (pagina şi inscripţia din registru);
c) numărul înregistrărilor efectuate;
d) tipul de acces;
e) data accesului (an, lună, zi);
f) timpul (ora, minuta) şi durata accesului

5.3. 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.

5.4. Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:
a) data şi timpul tentativei de pornire;
b) denumirea/identificatorul programului aplicativ sau al procesului;
c) ID-ul utilizatorului;
d) rezultatul tentativei de pornire – pozitivă sau negativă.

5.5. Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau 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.

5.6. Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:
a) data şi timpul modificării competenţelor;
b) ID-ul administratorului care a efectuat modificările;
c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

5.7. Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:
   a) data şi timpul eliberării;
   b) denumirea informaţiei şi căile de acces la aceasta;
   c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
   d) ID-ul utilizatorului care a solicitat informaţia;
   e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

5.8. În caz de deranjament al auditului securităţii în sistemul informaţional de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal şi sunt întreprinse măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit. Se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securităţii în sistemul informaţional de date cu caracter personal, în scopul depistării activităţilor neobişnuite sau suspecte de utilizare a acestor sisteme informaţionale, cu întocmirea raportului referitor la cazurile depistării acestor activităţi, stocate în mijloacele electronice de calcul, şi întreprinderea acţiunilor prestabilite în politica de securitate pentru astfel de cazuri.

5.9. Rezultatele auditului securităţii în sistemul informaţional de date cu caracter personal, care reprezintă operaţiuni de prelucrare a datelor cu caracter personal şi mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidenţialităţii şi integrităţii acestora. Durata stocării rezultatelor auditului securităţii în sistemul informaţional de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar, în orice caz, acest termen nu este mai mic de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

VI. ASIGURAREA INTEGRITĂŢII INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI A TEHNOLOGIILOR INFORMAŢIONALE

6.1. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor soft-uri, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsură care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

6.2. Se utilizează tehnologii şi mijloace de constatare a intrărilor ilegale, care permit monitorizarea evenimentelor şi constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemului informaţional de date cu caracter personal.

6.3. Se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemului informaţional de date cu caracter personal (automat - la pornirea sistemului şi lunar - la solicitarea utilizatorului autorizat în acest scop).

VII. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

7.1. Personalul care asigură exploatarea sistemului informaţional de date cu caracter personal trece minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

7.2. Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Incidentele de securitate a sistemului informaţional de date cu caracter personal se urmăresc şi se documentează în regim permanent.

7.3. Anual, către 31 ianuarie, deţinătorii de date cu caracter personal prezintă Centrului naţional pentru protecţia datelor cu caracter personal raportul generalizat despre incidentele de securitate a sistemului informaţional de date cu caracter personal din instituţie. În baza acestui raport, Centrul întreprinde măsurile ce se impun de Legea cu privire la protecţia datelor cu caracter personal

7.4. Persoanele împuternicite de către operator şi alte persoane vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia datelor personale ale salariaţilor din instituţie poartă răspundere disciplinară, materială, contravenţională şi penală în modul prevăzut de legislaţia în vigoare.

VIII. DISPOZIŢII FINALE

8.1. În temeiul dispoziţiilor art.91 alin.(1) lit.h) din Codul Muncii al Republicii Moldova, prezentul Regulament se aduce la cunoştinţa salariaţilor Institutului Naţional al Justiţiei, sub semnătură, de către Secția resurse umane și documentare, în termen de 10 zile lucrătoare de la data aprobării lui.

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