

REGULAMENT
privind protecția datelor cu caracter personal
ale salariaților din cadrul Institutului Național al Justiției

Sumar:

- I. Dispoziții generale privind datele cu caracter personal.
- II. Măsurile de protecție a datelor cu caracter personal și mecanismele de punere în aplicare a acestor măsuri.
- III. Securitatea și protecția sistemului informațional în procesul prelucrării datelor cu caracter personal.
- IV. Identificarea, autentificarea și administrarea accesului utilizatorului în sistemul informațional de date cu caracter personal.
- V. Auditul securității în sistemul informațional de date cu caracter personal.
- VI. Asigurarea integrității informației care conține date cu caracter personal și a tehnologiilor informaționale.
- VII. Gestionarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal.
- VIII. Dispoziții finale.

I. DISPOZIȚII GENERALE PRIVIND DATELE CU CARACTER PERSONAL

- 1.1. Prezentul Regulament dezvoltă și concretizează reglementările legale referitoare la modul, condițiile și procedurile de protecție a datelor cu caracter personal ale salariaților din cadrul Institutului Național al Justiției și este emis în calitate de act normativ la nivel de instituție 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 protecția datelor cu caracter personal nr.133 din 8 iulie 2011 și Hotărîrea Guvernului privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal nr.1123 din 14.12.2010.

1.3. Prezentele dispoziții, definesc următoarele noțiuni:

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

operator - persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;

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

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

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

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

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

politica de securitate a datelor cu caracter personal – document, elaborat de către deținătorul de date cu caracter personal, care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru securitatea datelor, ținându-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sînt expuse acestea;

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

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

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

tehnologie informațională ((TI) eng. - informational technologic) – totalitatea metodelor, procedurilor și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;

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

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

1.4. În componența datelor cu caracter personal se includ informațiile conținute în: buletinul de identitate sau un alt act de identitate, carnetul de muncă, documentele de evidență militară, certificatul medical, diploma de studii. La fel, pot fi raportate la categoria datelor cu caracter personal și datele autobiografice, informațiile despre salariu ș.a.

II. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL ȘI MECANISMELE DE PUNERE ÎN APLICARE A ACESTORA

2.1. Măsurile de protecție a datelor cu caracter personal prelucrate în sistemul informațional de date cu caracter personal se înfăptuiesc ținându-se cont de necesitatea asigurării confidențialității acestor măsuri, prin protecția datelor personale în formă manuală, electronică și externă.

2.1.1. Registrele în formă manuală - a angajaților, formatorilor și audienților INJ - se păstrează în Secția resurse umane și documentare, în safeul Secției.

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

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

- 2.1.3. Protecția externă a datelor personale ale salariatului se realizează prin: serviciul de pază, mijloace de signalizație sau alarmă antiincendiară.
- 2.2. Sînt supuse protecției toate resursele informaționale, care conțin date cu caracter personal, inclusiv:
 - a) suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
 - b) sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor, alte mijloace tehnice de prelucrare a informației.
- 2.3. Protecția datelor cu caracter personal în sistemul informațional este asigurată în scopul:
 - a) preîntîmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
 - b) preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resurselor informaționale;
 - c) respectării cadrului normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;
 - d) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în rețelele telecomunicaționale și resurselor informaționale;
 - e) păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.
- 2.4. Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:
 - a) preîntîmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
 - b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
 - c) preîntîmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
 - d) preîntîmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor angajați ai deținătorului de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program.
- 2.5. Preîntîmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, inclusiv cu utilizarea măsurilor organizaționale, tehnice și de regim, iar preîntîmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță.
- 2.6. Mecanismul de punere în aplicare a măsurilor de protecție este asigurat prin separarea posibilităților funcționale ale utilizatorului de posibilitățile funcționale de gestionare a

sistemelor informaționale, prin izolarea funcțiilor de securitate de funcțiile care nu se atribuie la securitatea acestui sistem și posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităților, a folosirii resurselor informaționale în care sînt prelucrate date cu caracter personal.

- 2.7. Se efectuează monitorizarea permanentă și controlul comunicațiilor la perimetrul exterior al sistemelor informaționale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaționale.
- 2.8. Este asigurată imposibilitatea accesului din exterior a utilizatorilor la rețeaua internă în care se prelucrează date cu caracter personal, totodată asigurîndu-se integritatea și confidențialitatea datelor cu caracter personal transmise prin utilizarea mijloacelor de protecție criptografică a informației și semnătura digitală.

III. SECURITATEA ȘI PROTECȚIA SISTEMULUI INFORMAȚIONAL ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

- 3.1. Prezentul Regulament se revizuieste cel puțin o dată în an, ca rezultat al modificărilor sau reevaluării componentelor acestuia și aprobat la cel mai înalt organ suprem de conducere al instituției – Consiliul INJ.
- 3.2. Directorul executiv numește prin ordin (Anexa 1) o persoană responsabilă de elaborarea, implementarea și monitorizarea respectării prevederilor Regulamentului privind protecția datelor cu caracter personal care vizează salariații din cadrul INJ, subordonată nemijlocit directorului instituției, care nu va avea alte responsabilități incompatibile cu sarcinile funcției 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 și buget) și va avea acces liber la informația necesară pentru îndeplinirea funcțiilor sale în măsura în care acestea nu operează în afara cadrului acestei politici, totodată va avea diferite responsabilități cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare și prelucrare), precum și operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.
- 3.4. Accesul în sediile/birourile ori spațiile unde sînt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară- Directorul executiv, Directorul executiv adjunct, contabilul șef și șeful Serviciului resurse umane și documentare - și doar în timpul orelor de program, conform listei și însemnelor corespunzătoare -insigne, ecusoane, cartele de identificare, cartele cu microprocesoare.
- 3.5. Se efectuează administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces și competențele de acces. Acordarea accesului fizic la sistemele informaționale de date cu caracter personal se face prin registrele de monitorizare, care se păstrează minimum un an, la expirarea cărui acestea se lichidează, iar datele și documentele ce se conțin 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 și trebuie să fie integrat din punct de vedere fizic. Pereții exteriori ai încăperilor trebuie să fie rezistenți, intrările

echipate cu lacăte, mijloace de control al accesului, semnalizare etc. În cazul amplasării încăperilor la parter și/sau la ultimul etaj al clădirii, precum și în cazul existenței 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. Ușile și ferestrele se încuie în cazul în care în încăperea lipsesc angajații. Agendele și/sau cărțile de telefoane în care se conțin 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 necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței unei permisiuni speciale a conducerii deținătorului de date cu caracter personal. Purtătorii de informații și 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 menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, trebuie asigurată posibilitatea deconectării electricității la sistemele informaționale 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 comunicaționale pentru a exclude bruiatul.
- 3.9. Deținătorii 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 rețea. Se prevăd mijloace de asigurare a securității antiincendiare a sediilor/oficiilor/birourilor unde sînt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal. Se exercită controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.
- 3.10. Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitîndu-se folosirea funcțiilor standard de nimicire. În cazul neutilizării temporare a purtătorilor de informație pe suport de hîrtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.
- 3.11. Computerele, terminalele de acces și imprimantele sînt deconectate la terminarea sesiunilor de lucru. Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere. Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii deținătorului de date cu caracter personal. Scoaterea și introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează.

IV. IDENTIFICAREA, AUTENTIFICAREA ȘI ADMINISTRAREA ACCESULUI UTILIZATORULUI ÎN SISTEMUL INFORMAȚIONAL DE DATE CU CARACTER PERSONAL

- 4.1. Se implementează mecanisme de înregistrare și evidență a persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal și care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.
- 4.2. Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmamentele 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 și individuale ale persoanei.
- 4.3. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă sau se suspendă de către deținătorul 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 și ștergerea acestora. Sînt folosite mijloace automatizate de suport în scopul administrării conturilor de acces. Acțiunea 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 și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.
- 4.5. Este autorizat accesul la sistemele informaționale de date cu caracter personal în conformitate cu politica de administrare a accesului stabilită de deținătorul de date cu caracter personal. Accesul la funcțiile de securitate ale sistemului informațional de date cu caracter personal și la datele acestora este acordat doar persoanelor responsabile indicate expres în politica de securitate a deținătorului de date cu caracter personal. Drepturile de acces ale utilizatorilor la sistemul informațional de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare șase luni) și după oricare schimbare de statut al utilizatorului.
- 4.6. Se autorizează de către deținătorii de date cu caracter personal realizarea fluxurilor informaționale în procesul transmiterii acestora în interiorul și în afara sistemului informațional de date cu caracter personal. Accesul fără fir la sistemul informațional de date cu caracter personal este documentat, supus monitorizării și controlului și este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației. Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale deținătorului de date cu caracter personal.

V. AUDITUL SECURITĂȚII ÎN SISTEMELE INFORMAȚIONALE DE DATE CU CARACTER PERSONAL

- 5.1. Deținătorii de date cu caracter personal organizează generarea înregistrărilor de audit a securității în sistemul informațional de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.
- 5.2. Înregistrările de audit a securității registrelor ținute manual în care sînt prelucrate date cu caracter personal, trebuie să conțină:
 - a) numele și prenumele utilizatorului;
 - b) numele fișei accesate (pagina și inscripția din registru);
 - c) numărul înregistrărilor efectuate;
 - d) tipul de acces;
 - e) data accesului (an, lună, zi);
 - f) timpul (ora, minuta) și durata accesului
- 5.3. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
 - a) data și timpul tentativei intrării/ieșirii;
 - b) ID-ul utilizatorului;
 - c) rezultatul tentativei de intrare/ieșire – pozitivă sau negativă.
- 5.4. Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:
 - a) data și 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 obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
 - a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
 - b) denumirea (identificatorul) aplicației sau a procesului;
 - c) ID-ul utilizatorului;
 - d) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
 - e) tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
 - f) rezultatul tentativei de obținere a accesului (executare a operațiunii) – pozitivă sau negativă.
- 5.6. Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
 - a) data și timpul modificării competențelor;
 - b) ID-ul administratorului care a efectuat modificările;
 - c) ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

- 5.7. Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
- a) data și timpul eliberării;
 - b) denumirea informației și căile de acces la aceasta;
 - c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
 - d) ID-ul utilizatorului care a solicitat informația;
 - e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.
- 5.8. În caz de deranjament al auditului securității în sistemul informațional 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 și sunt întreprinse măsuri în vederea restabilirii capacității de lucru a sistemului de audit. Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemul informațional de date cu caracter personal, în scopul depistării activităților neobișnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul, și întreprinderea acțiunilor prestabilite în politica de securitate pentru astfel de cazuri.
- 5.9. Rezultatele auditului securității în sistemul informațional de date cu caracter personal, care reprezintă operațiuni de prelucrare a datelor cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității și integrității acestora. Durata stocării rezultatelor auditului securității în sistemul informațional 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 investigații sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

VI. ASIGURAREA INTEGRITĂȚII INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI A TEHNOLOGIILOR INFORMAȚIONALE

- 6.1. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestor soft-uri, protecția contra infiltrării programelor dăunătoare în soft-uri, măsură care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.
- 6.2. Se utilizează tehnologii și mijloace de constatare a intrărilor ilegale, care permit monitorizarea evenimentelor și constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemului informațional de date cu caracter personal.
- 6.3. Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemului informațional de date cu caracter personal (automat - la pornirea sistemului și lunar - la solicitarea utilizatorului autorizat în acest scop).

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

- 7.1. Personalul care asigură exploatarea sistemului informațional 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.
- 7.2. Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Incidentele de securitate a sistemului informațional de date cu caracter personal se urmăresc și se documentează în regim permanent.
- 7.3. Anual, către 31 ianuarie, deținătorii de date cu caracter personal prezintă Centrului național pentru protecția datelor cu caracter personal raportul generalizat despre incidentele de securitate a sistemului informațional de date cu caracter personal din instituție. În baza acestui raport, Centrul întreprinde măsurile ce se impun de Legea cu privire la protecția datelor cu caracter personal
- 7.4. Persoanele împuternicite de către operator și alte persoane vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția datelor personale ale salariaților din instituție poartă răspundere disciplinară, materială, contravențională și penală în modul prevăzut de legislația în vigoare.

VIII. DISPOZIȚII FINALE

- 8.1. În temeiul dispozițiilor art.91 alin.(1) lit.h) din Codul Muncii al Republicii Moldova, prezentul Regulament se aduce la cunoștința salariaților Institutului Național al Justiției, sub semnătură, de către Secția resurse umane și documentare, în termen de 10 zile lucrătoare de la data aprobării lui.
- 8.2. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.