

**MINISTERUL EDUCAȚIEI AL REPUBLICII MOLDOVA
UNIVERSITATEA DE STAT DIN MOLDOVA**

Aprobat
Prin decizia Senatului Universității de Stat
din Moldova, din 28.04.2015.

**POLITICA DE SECURITATE
PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL LA
PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR
INFORMAȚIONALE GESTIONATE DE UNIVERSITATEA DE STAT DIN
MOLDOVA (USM)**

DISPOZIȚII GENERALE

Prezenta „Politică de securitate a prelucrării datelor cu caracter personal” a fost elaborată în conformitate cu prevederile legislației naționale în vigoare, inclusiv a Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal și prevederile Hotărârii Guvernului Republicii Moldova nr.1123 din data de 14 decembrie privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal și reglementează modul în care sunt colectate și utilizate aceste informații, precum și condițiile de utilizare a informației în cadrul Universității de stat din Moldova.

Semnificațiile termenilor și noțiunilor utilizate în prezenta Politică de Securitate:

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 constrângere sau sancțiunile contravenționale;

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 identificadorului atribuit subiectului de acces, confirmarea autenticității;

control de securitate – acțiuni întreprinse de către USM în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;

fișiere temporare – ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat pînă la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare – atribuirea unui identificador subiecților și obiectelor de acces și/sau compararea identificadorului 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;

nivel de protecție – nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor, elaborat și actualizat corespunzător nivelului dezvoltării tehnologice și costurilor implementării acestor măsuri;

politica de securitate a datelor cu caracter personal – document, elaborat de către operatorul de date USM 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;

protecția informației contra acțiunilor neintenționate – ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține 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;

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 informațională – totalitatea metodelor, procedeelor 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;

sesiune de lucru – perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și pînă la momentul opririi acestora;

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;

prelucrarea datelor cu caracter personal – orice operațiune sau serie de operațiuni 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, ștergerea sau distrugerea;

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

sistem de evidență 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 criteriile funcționale sau geografice;

consimțămîntul subiectului datelor cu caracter personal – orice manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor 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 circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă.

POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

Deținătorii de date cu caracter personal, reieșind din specificul activității, elaborează și organizează implimentarea prevederilor documentului care stabilește politica de securitate a datelor cu caracter personal, inclusiv procedurile și măsurile legate de realizarea acestei politici, cu aplicarea soluțiilor practice cu un nivel de detalizare și complexitate proporțional, în partea ce ține de identificarea și autentificarea utilizatorilor.

Politica de securitate și obiectivele principale ale politicii de securitate sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal, atît în cadrul prelucrării manuale, cît și sistemelor informaționale.

Persoanele împuternicite de către operator vor asigura protecția datelor cu caracter personal prin aplicarea corespunzătoare a legislației în vigoare cu referire la protecția datelor și confidențialitatea comunicării.

Politica de securitate, în mod obligatoriu va fi adusă la cunoștință sub semnătură tuturor angajaților responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv și la

operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecție a datelor cu caracter personal.

Prevederile Politicii de Securitate și regulilor interne ale USM ce vizează protecția datelor cu caracter personal urmează să fie respectate strict de către toți salariații Universității de Stat din Moldova.

DISPOZIȚII PRIVIND OBLIGAȚIILE PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE

Responsabil de implementarea și monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, va fi persoana desemnată prin ordinul rectorului care va dispune de resurse suficiente (timp, resurse umane 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.

Persoana responsabilă desemnată, indiferent de funcțiile exercitate în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit rectorului USM sau persoanei care îndeplinește interimatul funcției.

Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferențelor responsabilității cu privire la securitatea prelucrării datelor cu caracter personal (prevenirea, supravegherea, detectarea și prelucrarea), precum și operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

Persoana responsabilă de politica de securitate a datelor cu caracter personal va defini clar responsabilitățile și procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională și de funcționare generală, va asigura măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal.

Persoana responsabilă de politica de securitate a datelor cu caracter personal va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către aceștea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Prelucrarea datelor cu caracter personal se realizează în temeiul și în conformitate cu prevederile legale în vigoare ale Republicii Moldova.

Prelucrarea datelor cu caracter personal se realizează în scopuri bine determinate, explicite și legitime, adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate.

Prelucrarea datelor cu caracter personal, cu excepția prelucrărilor strict menționate în Legea nr.133 din 08.07.2011 cu privire la datele cu caracter personal,

poate fi efectuată numai dacă persoana vizată și-a dat consimțământul în mod expres și neechivoc pentru acea prelucrare.

Refuzul subiectului pentru prelucrarea acestor date se echivalează cu imposibilitatea executării contractului de muncă.

MĂSURI DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul informațional de date cu caracter personal, se îndeplinesc ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică și externă.

Măsurile de protecție a datelor cu caracter personal sunt asigurate în scopul:

- a) preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la acestea;
- b) preîntâmpinării distrugerii, modificării, copierii;
- c) respectării cadrului normativ de operare a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;
- d) asigurării caracterului complet, integru și verdict al datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
- e) asigurării posibilității de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal;
- f) preîntâmpinării conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- g) excluderii accesului neautorizat la datele cu caracter personal prelucrate;
- h) preîntâmpinării acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul sistemului tehnic și de program;
- i) preîntâmpinării acțiunilor intenționate și/sau neintenționate ale utilizatorilor interni și/sau externi, precum și ale altor deținători de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul sistemului tehnic și de program.

Preîntâmpinarea scurgerii informației care conține 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 preîntâmpinarea 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.

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 sunt prelucrate datele cu caracter personal.

SECURITATEA MEDIULUI FIZIC ȘI PROTECȚIA SISTEMULUI INFORMAȚIONAL ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Accesul în oficiile și birourile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program, cu înregistrarea în registrul de evidență a timpului de muncă.

Se administrează și monitorizează accesul fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv reacționează la încălcarea regimului de acces și competențelor de acces. Acordarea accesului fizic la sistemele informaționale de date cu caracter personal se face prin registrele de monitorizare, care se păstrează minim un an, la expirarea cărui acestea se lichidează, iar datele și documentele ce se conțin în registru supus lichidării se transmit în arhivă.

Perimetrul de securitate al încăperilor în care sunt amplasate baza de date și mijloacele de prelucrare a datelor cu caracter personal este integrat din punct de vedere fizic. Pereții exteriori ai încăperilor sunt rezistenți, intrările echipate cu lacăte, mijloace de control, semnalizare etc.

Oficiile și birourile unde sînt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal sunt dotate cu mijloace de asigurare a securității antiincendiare.

Folosirea tehnicii foto, audio, video sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar cu acordul special al rectorului sau prorectorului universității. Purtătorii de informații și mijloacele de prelucrare a datelor cu caracter personal scoase din încăperi aflate în perimetrul de securitate nu trebuie lăsate fără supraveghere în locuri publice.

Deținătorii de date cu caracter personal efectuează controale, nu mai rar decît o dată în lună, în scopul verificării cazurilor de conectare neautorizate la cablurile de rețea.

Informațiile care conțin date cu caracter personal și care se conțin pe purtători de informație, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitîndu-se folosirea funcțiilor standarde de nimicire. În cazul neutilizării temporare a purtătorilor de informații pe suport de hîrtie sau electronice (digital) care conține date cu caracter personal, acestea se păstrează în safeuri care se încuie.

Operatorul va asigura securitatea echipamentului electric utilizat pentru menținerea funcționalității informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorării și conectărilor nesancționate.

Oficiile și birourile unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal sunt dotate cu mijloace de asigurare a securității antiincendiare.

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.

Operatorul va prezenta anual, către 31 ianuarie Centrului Național pentru Protecția Datelor cu Caracter Personal raportul generalizat despre incidentele de securitate a sistemelor informaționale de date cu caracter personal.

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

În scopul identificării cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal, operatorul înregistrează și se duce evidența persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal.

Sistematic se efectuează controlul acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

În scopul identificării cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal se înregistrează și se duce evidența persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal.

Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea sistemelor informaționale de date cu caracter personal este controlată și că folosirea neautorizată a acestora se urmărește în conformitate cu legislația.

Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea parolelor pe suport de hîrtie, cu excepția cazului de asigurare a securității păstrării acesteia. La momentul introducerii, parolele nu se reflectă în clar pe monitor. Persoanele împuternicite de către operator vor modifica parolele de fiecare dată cînd va depista indici ai unei eventuale compromiteri a sistemului sau parolei.

Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sunt folosite identificarea și parole individuale ale acestora. Se asigură utilizatorilor posibilitatea de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora. După trei tentative greșite de autentificare accesul este blocat.

Operatorul asigură, pentru o perioadă de 1 /un / an păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor și prevenirea folosirii repetate a acestora.

În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, și ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum și în cazul de modificare a drepturilor de acces ale utilizatorului, abuz a utilizatorului de codurile permise în scopurile comiterii unei fapte prejudiciabile, absență a utilizatorului pe parcursul unei perioade îndelungate, codurile de identificare și autentificarea se revocă sau se suspendă.

În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuite cu regularitate, maximum peste fiecare șase luni și după oricare

schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul informațional de date cu caracter personal.

AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ SECȚIA RESURSE UMANE

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

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.

Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din sistemul automatizat de, 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.

Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din sistemul automatizat de, 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.

Se efectuează 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.

Se efectuează înregistrarea ieșirii din sistemul automatizat de evidență, 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, filelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.

Cazurile de deranjament al auditului securității în sistemul automatizat de evidență sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoștința persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

Rezultatele auditului securității în sistemul automatizat de evidență a (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

ASIGURAREA INTEGRITĂȚII INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ

Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din sistemul automatizat de evidență a, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestora, protecția contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.

Se utilizează tehnologii și mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor și constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informațiilor din sistemul automatizat de evidență a salariaților.

Se asigură testarea funcționării corecte a componentelor de securitate a sistemului automatizat de evidență a salariaților (automat – la pornirea sistemului, și după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

Copiile de siguranță: reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către operator intervalul de timp în care se execută copiile de siguranță a informațiilor din sistemul de evidență a salariaților și soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ

Persoanele care asigură exploatarea sistemul automatizat de evidență trec, minimum o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență.

Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din sistemul de evidență poartă răspundere civilă, contravențională și penală.

DREPTURILE SUBIECȚILOR DE DATE CU CARACTER PERSONAL

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

- a) privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registru de evidență al operatorului de date cu caracter personal);
- b) privind scopul concret al prelucrării datelor cu caracter personal colectate;
- c) privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- d) existența drepturilor la informarea 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.

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 neincluserii 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.

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

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.

DEZVĂLUIREA DATELOR CU CARACTER PERSONAL

Dezvăluirea formatului electronic al datelor cu caracter personal conținute în sistemele de evidență, prin rețele comunicaționale ori prin alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidență a datelor cu caracter personal este permis doar utilizatorilor autorizați.

Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice asigurate de destinatar și operator, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere (expediere poștală cu aviz recomandat, înmînarea personală, etc.).

Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce corespund Cerințelor, (de exemplu: expedierea informației prin intermediul e-mail-urilor personale de tip @gmail.com, @mail.ru, @yahoo.com, etc.) sunt interzise.

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 adevărate circumstanțe care au importanță pentru cauză, (inclusiv informația stocată în auditul sistemelor informaționale și 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 și 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 cunoștință cu fișa personală a clientului, aceștia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art. 15 Cod de Procedură Penală, art. 29 și 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art.74¹ Cod Contravențional.

**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, semnatarii a anexei nr.1, pentru nerespectarea dispozițiilor Politicii de securitate poartă răspundere civilă (Cod Civil), contravențională (art.74¹ Cod Contravențional) și penală (art. 177, 178, 180 Cod Penal).