Anexa nr. 1
Aprobat prin Ordinul *nr. 131 G*
din 07 octombrie 2022

POLITICA DE SECURITATE
PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL
ȘI PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR
INFORMAȚIONALE ADMINISTRATE DE
INSTITUȚIA PUBLICĂ ORGANIZAȚIA PENTRU DEZVOLTAREA ANTREPRENORIATULUI

Cuprins

I. Dispoziții generale

Politica de securitate privind protecția datelor cu caracter personal stabilește modul, condițiile și procedurile de protecție a datelor cu caracter personal în cadrul Instituției Publice Organizația pentru Dezvoltarea Antreprenorialului (*în continuare IP ODA*) și urmează a fi aprobată de către Directorul IP ODA.

Politica are la bază prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal, Hotărârii Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, dar și prevederile Regulamentului 679/2016 al Parlamentului European.

II. Noțiuni generale

În prezenta Politică de Securitate, sunt 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 constrângere sau sancțiunile contravenționale.

date biometrice - date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

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.

parte terță - persoană fizică sau juridică, autoritate publică, agenție sau organism ,altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

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.

prelucrarea - 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 criterii funcționale sau geografice.

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.

creare de profiluri - orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul etc.

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

integritate - certitudinea, ne-contradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată.

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 sunt expuse acestea.

persoană responsabilă de protecția datelor — 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.

control de securitate - acțiuni întreprinse de către deținătorii de date cu caracter personal în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute.

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.

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

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.

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

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.

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.

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

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

consimţământul 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 încât detaliile privind circumstanţele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condiţiile unei investigaţii care necesită cheltuieli disproporţionate de timp, mijloace şi forţă de muncă.

încălcarea securităţii datelor cu caracter personal – încălcare a normelor de securitate care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

III. Obiectivele Politicii de Securitate

1. Obiectivele principale ale Politicii de securitate sunt asigurarea integrității și confidențialității tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de IP ODA, atât în cadrul prelucrării manuale, cât și prin intermediul tehnologie informațională.

2. Asigurarea unui nivel minim de securitate are ca scop derularea optimă a proceselor bazate pe tehnologii informaționale în cadrul IP ODA. Politica cuprinde cerințele și regulile care au ca scop protecția tuturor informațiilor (informații confidențiale, date cu caracter personal etc) și proceselor IT împotriva influențelor naturale, erorilor umane și tehnice.

3. IP ODA va proteja datele cu caracter personal atât a participanților la proces/vizitatori, cât și a salariaților săi.

4. Pornind de la această reglementare, toți salariații IP ODA urmează să respecte strict prevederile Politicii și regulilor interne ale IP ODA privind protecția datelor cu caracter personal și sistemelor IT.

IV. Persoana responsabilă de Politica de securitate

1. IP ODA, în calitate de operator de date cu caracter personal, reieșind din specificul activității, prin prezenta Politică de securitate, transpune procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență gestionate.

2. Politica de securitate a datelor cu caracter personal va fi revizuită ori de câte ori este nevoie, ca rezultat al modificărilor sau reevaluării competențelor entității. Conducătorii instituției sunt responsabili de desemnarea persoanei responsabile de ajustarea prevederilor prezentului act.

3. 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.

4. Responsabil de implementarea și monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, va fi desemnată persoana care conform fișei postului și/sau ordinului intern, 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 aceasta nu operează în afara cadrului acestei politici.

5. Persoana responsabilă desemnată, indiferent de funcțiile exercitate, în cadrul procesului de monitorizare a implementării si respectării politicii de securitate, se va subordona nemijlocit Directorului IP ODA.

6. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor 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.

7. Persoana responsabilă de politica de securitate a datelor cu caracter personal va defini clar responsabilitățile și procesele de management a securității datelor cu caracter personal cu

integrarea lor corespunzătoare în structura organizațională, va asigura măsurile tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal, fiindu-i acordat suport de către Secția suport și securitate IT, în limita competențelor.

8. Persoana responsabilă de politica de securitate a datelor cu caracter personal va elabora procedurile de clasificare a informației care conține date cu caracter personal și/sau confidențial, astfel încât să fie posibilă întocmirea unui nomenclator pentru localizarea eficientă a datelor prelucrate.

9. 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 acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal inclusiv a confidențialității acestora.

V. Mijloacele de protecție a datelor cu caracter personal

1. Protecția datelor cu caracter personal în cadrul IP ODA (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnico-organizatorice care au ca scop prevenirea scurgerii și/sau prelucrării ilicite de date cu caracter personal.

2. Sunt supuse protecției toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate pe:

a) suporturi 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 și alte mijloace tehnice de prelucrare a informației.

VI. Măsuri de protecție

Măsurile de protecție a datelor cu caracter personal prelucrate în sistemele informaționale în cadrul IP ODA sunt:

1. Prevenirea scurgerii de date cu caracter personal prin metoda excluderii accesului neautorizat.

2. Prevenirea acțiunilor speciale tehnice și de program, care pot duce la distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

3. Prevenirea conexiunilor neautorizate în cadrul rețelelor de telecomunicații și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;

4. Prevenirea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

5. Preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea canalelor VPN;

6. Preîntâmpinarea distrugerii, modificării sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin folosirea mijloacelor de protecție 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;

7. Preîntâmpinarea scurgerii de informații ce conțin date cu caracter personal, este asigurată prin intermediul auditului intern al sistemelor informaționale, care se efectuează permanent.

VII. Procedurile organizatorice și tehnice

1. Măsurile generale de administrare a securității informaționale:

a) Salariații, în cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, urmează să îi păstreze în safeuri sau dulapuri care se încuie.

b) Salariații sunt obligați să deconecteze computerele, terminalele de acces și imprimantele la terminarea sesiunilor de lucru.

c) Salariații asigură securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.

d) Salariații sunt obligați să restricționeze accesul fizic neautorizat la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

e) Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal pot fi scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise din partea superiorului ierarhic sau a persoanei responsabile de protecția datelor cu caracter personal.

f) Toate programele utilizate în cadrul sistemului informațional trebuie să respecte condițiile de licențiere și urmează să fie aprobate de către Secția suport și securitate IT.

g) Secția suport și securitate IT urmează să aprobe instalarea și/sau utilizarea programelor de tip Shareware sau Freeware.

1. Măsurile de asigurare a securității mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal:

a) Accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este permis doar persoanelor care au autorizația necesară, aceasta fiind oferită de către responsabilul de protecția datelor.

b) Accesul persoanelor terțe în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal se efectuează doar cu supravegherea permanentă a acestora de către unul sau mai mulți angajați. Salariații trebuie să se asigure că, în spațiul dat nu există suporturi care conțin date cu caracter personal în locuri vizibile.

c) Persoana responsabilă de protecţia datelor cu caracter personal asigură administrarea şi monitorizarea accesului fizic în punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv reacţionează prompt la încălcarea regimului de acces.

d) Perimetrul de securitate al IP ODA urmează să fie delimitat prin punctele securizate de acces fizic şi reprezintă perimetrul oficiilor în care sunt prelucrate/stocate date cu caracter personal.

e) Perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal trebuie să îşi păstreze integritatea din punct de vedere fizic, pereţii exteriori ai încăperilor trebuie să fie rezistenţi, iar intrările echipate cu lacăte şi semnalizare.

f) Persoana responsabilă de protecţia datelor cu caracter personal urmăreşte ca amplasarea mijloacelor de prelucrare a datelor cu caracter personal să corespundă necesităţii asigurării securităţii acestora contra accesului neautorizat, furturilor, incendiilor şi altor posibile riscuri.

g) Uşile urmează să fie încuiate de către salariaţi, în cazul în care aceştia lipsesc din încăpere.

g) Secţia suport şi securitate IT este responsabilă ca serverele, computerele şi alte terminale de acces să fie amplasate în locuri cu acces limitat pentru persoanele străine.

h) Accesul în perimetrul de securitate al IP ODA cu utilaje foto/video neautorizate este interzis, ţinând 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.

i) 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 organizaţiei.

2. Identificarea şi autentificarea utilizatorilor.

a) Identificarea şi autentificarea utilizatorilor în sistemele informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori se efectuează prin introducere login-ului şi parolei.

b) Secţia suport şi securitate IT urmează să atribuie tuturor utilizatorilor (inclusiv personalului care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) un identificator personal (ID-ul utilizatorului), care nu conţine semnalmentele nivelului de accesibilitate al utilizatorului.

c) Pentru confirmarea ID-ului, utilizatorii utilizează parole, mijloace fizice speciale de acces cu memorie (token) sau mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.

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 de către salariaţii din secţia suport şi securitate IT şi/sau responsabilul de protecţia datelor cu caracter personal.

4. Administrarea identificatorilor utilizatorilor se efectuează prin:

a) identificarea univocă a fiecărui utilizator.

b) verificarea autenticităţii fiecărui utilizator.

5. Utilizarea parolelor în procesul asigurării securității informaționale:

a) Fiecare salariat IP ODA este responsabil de păstrarea confidențialității parolelor.
b) Se interzice înscrierea parolelor de către salariați pe suport de hârtie,.
c) Salariații trebuie să își modifice parolele cel puțin o data la 3 luni și de fiecare dată când sunt prezente indiciile unei eventuale compromiteri a sistemului sau a parolei.
d) Salariații trebuie să aleagă o parolă de minimum 8 simboluri (care să conțină litere, cifre și alte simboluri), care nu sunt legate de informația cu caracter personal a utilizatorului.
e) Este interzisă utilizarea de către salariați a procesului automatizat de înregistrare (cu folosirea parolelor salvate).

6. Controlul administrării accesului

Secția suport și securitate IT este responsabilă de efectuarea controlului sistematic al acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

7. Accesul de la distanță

a) Secția suport și securitate IT, în colaborare cu persoana responsabilă de protecția datelor cu caracter personal, urmează să securizeze (utilizând VPN, criptarea, cifrarea), să documenteze, să monitorizeze și să controleze toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal.
b) Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este autorizată de persoanele responsabile din cadrul IP ODA.

8. Limitarea folosirii tehnologiilor fără fir (prin WIFI)

a) Secția suport și securitate IT va limita accesul fără fir la sistemele informaționale de date cu caracter personal.
b) Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar salariaților care utilizează mijloace criptografice de protecție a informației.
c) Folosirea tehnologiilor fără fir de către salariați se autorizează de persoanele responsabile din cadrul IP ODA.

9. Securitatea electroenergetică

a) Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesancționate, prin montarea lor în nișe speciale.
b) Administrația clădirii și/sau Secția Resurse Umane se obligă ca în cazul apariției situațiilor excepționale, de avarie sau de forță majoră, să asigure cât mai rapid posibil deconectarea

electricității la sistemele informaționale de date cu caracter personal, inclusiv deconectarea oricărui component IT.

c) Secția suport și securitate IT, împreună cu persoana responsabilă de protecția datelor cu caracter personal se obligă se implementeze sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.
d) Secția suport și securitate IT, împreună cu persoana responsabilă de protecția datelor cu caracter personal se obligă să distrugă fizic sau să transcrie și să nimicească prin metode sigure datele cu caracter personal care se conțin pe purtători de informații, evitându-se folosirea funcțiilor standarte de nimicire.

10. Dezvăluirea datelor cu caracter personal

a) 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 trebuie efectuat în corespundere cu măsurile organizatorice și tehnice implementate de părți. În cazul în care rețelele comunicaționale prezintă riscuri care pot afecta confidențialitatea și securitatea datelor cu caracter personal, utilizatorii se obligă să folosească metode tradiționale de transmitere (expediere poștală cu aviz recomandat, înmânarea personală, etc.).
b) Se interzice dezvăluirea prin transmitere a datelor cu caracter personal, utilizând rețele comunicaționale ce nu corespund cerințelor (spre exemplu: expedierea informației prin intermediul e-mail-urilor personale, rețele sociale, etc).
c) Sunt interzise operațiunile de dezvăluire a datelor cu caracter personal între IP ODA și alte entități care sunt amplasate geografic în stânga Nistrului, care refuză să se supună juridic legislației Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal.
d) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hârtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luându-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal.
e) Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecția datelor cu caracter personal, în special în cazurile când tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal.
f) Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței IP ODA, este limitat la strictul necesar pentru realizarea scopurilor declarate.
g) Accesul la sistemele informaționale gestionate în cadrul IP ODA, din partea Procuraturii General (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 și art. 212 Cod de procedură penală.

h) 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 sunt expuse ori adeverite circumstanțe care au importanță pentru cauză, (inclusiv informația stocată în auditul sistemelor informaționale și de evident(ă), 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 răspândite 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.

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. 74 [1] Cod contravențional.

VIII. 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 urmează să i se furnizeze următoarele informații, exceptând cazul în care el deține deja informațiile respective:

a) identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul);

b) scopul concret al prelucrării datelor cu caracter personal colectate;

c) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

d) 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

condiţiile în care aceste drepturi pot fi exercitate, dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia.

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

f) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entităţile ce asigură mentenanţa sistemului sau prestează servicii externalizare ale operatorului) tuturor persoanelor supuse prelucrării.

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

IX. Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate

a) Accesul în spaţiile/perimetrul unde sunt amplasate sistemele informaţionale şi de evidenţă a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară conform politicii de securitate instituţionale /regulamentelor departamentale aprobate.

b) Stocarea şi păstrarea în format electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sunt conectate la internet, dar care nu sunt supuse efectuării copiilor periodice sau auditului este interzisă.

c) Accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredinţate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul IP ODA.

d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie.

e) Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

X. Auditul sistemelor informaționale gestionate

a) Secția suport și securitate IT efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

- data și timpul tentativei intrării/ieșirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieșire: pozitivă sau negativă.

b) Secția suport și securitate IT. efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- data și timpul tentativei de obținere a accesului (executate a operațiunii).
- denumirea (identificatorul) aplicației sau procesului.
- ID-ul utilizatorului.
- specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.)
- tipul operațiunii solicitate (citire, înregistrare, ștergere etc.).
- rezultatul tentativei de obținere a accesului (executare a operațiunii) — pozitivă sau negativă.

c) Secția suport și securitate IT efectuează înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

- data și timpul modificării competențelor.
- ID-ul administratorului care a efectuat modificările.
- ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

d) Secția suport și securitate IT 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:

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

XI. Asigurarea protecției contra programelor dăunătoare (virușilor)

- Secția suport și securitate IT asigură protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existența programelor licențiate anti-virus.

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

Secţia suport şi securitate IT asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal.

XIII. Gestionarea incidentelor de securitate

a) Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal este obligat să treacă, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

b) Salariaţii sunt obligaţi să informeze neîntârziat conducerea IP ODA despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

c) Prelucrarea incidentelor se efectuează de persoana responsabilă de protecţia datelor cu caracter personal în colaborare cu Secţia suport şi securitate IT şi include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii

d) În cazul producerii incidentelor de securitate în cadrul instituţiei, persoana responsabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova.

XIV. Responsabilitatea pentru asigurarea securităţii datelor cu caracter personal, precum şi a informaţiilor cu accesibilitate limitată

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terţe – pentru nerespectarea dispoziţiilor Politicii de securitate, poartă răspundere civilă (Codul civil), contravenţională (art. 74^1 Cod contravenţional) şi penală (art. 177, 178, 180 Cod penal).

Director interimar D. Pîntea **Dumitru PÎNTEA**