Anexa nr. 1
La Decizia nr. 5 din 14.07.2021

Politica de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de către Agenția pentru Dezvoltarea și Modernizarea Agriculturii

Secțiunea I. Dispoziții generale

1. Prelucrarea datelor cu caracter personal în cadrul Agenției pentru Dezvoltarea și Modernizarea Agriculturii se realizează în baza principiilor prevăzute de Declaraţia universală a drepturilor omului, Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale, Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal și a celor naționale – Constituția Republicii Moldova, Legea nr. 133/2011 privind protecția datelor cu caracter personal, Legea nr. 982/2000 privind accesul la informație, Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr. 1123/2010, Regulamentului Registrului de evidenţă al operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr. 296/2012 și alte acte normative relevante.
2. În prezenta Politică de securitate, sînt definite/utilizate următoarele noţiuni:
   a) *date cu caracter personal* – orice informaţie 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 identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;
   b) *categorii speciale de date cu caracter personal* – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenenţa socială, datele privind starea de sănătate sau viaţa sexuală, precum şi cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancţiunile contravenţionale;
   c) *operator* – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituţie ori organizaţie care, în mod individual sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislaţia în vigoare;
   d) *persoană împuternicită de către operator* – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor primite de la operator;
   e) *autentificare* - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;
   f) *control de securitate* - acţiuni întreprinse de către(operator) ADMA în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute;
   g) *fişiere temporare* - ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat pînă la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;
   h) *identificare* - atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;
   i) *integritate* - certitudinea, necontradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;
   j) *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;
   k) *nivel de protecţie* - nivel de securitate proporţional riscului pe care îl comportă prelucrarea faţă de datele cu caracter personal respective, precum şi faţă de drepturile şi libertăţile persoanelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri;

l) *politica de securitate a datelor cu caracter personal* - document, elaborat de către operatorul de date Agenţia pentru Dezvoltarea şi Modernizarea Agriculturii (în continuare Agenţie), care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinîndu-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sînt expuse acestea;

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

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

o) *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;

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

q) *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;

r) *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;

s) *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;

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

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

v) *prelucrarea datelor cu caracter personal* – orice operaţiune sau serie de operaţiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;

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

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

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

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

Secţiunea II. Obiectivele politicii de securitate

3. Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de Agenție, atît în cadrul prelucrării manuale, cît și prin intermediul sistemelor și proceselor de tehnologie informațională.
4. Securitatea reprezintă o componentă esenţială a derulării optime a proceselor bazate pe tehnologia informațională (în continuare IT) a Agenției. Baza unei securităţi IT adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datele cu caracter personal, sistemelor şi proceselor IT împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației. Avînd în vedere că siguranţa IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic.
5. Agenția va proteja datele cu caracter personal atît a participanților la proces/vizitatori, cît și a angajaților săi.
6. Reglementările prezentei Politici de securitate reprezintă un standard minim pentru Agenție. Pornind de la această reglementare, angajații Agenției urmează să respecte strict prevederile privind protecția datelor cu caracter personal și sistemelor IT.

Secțiunea III. Dispoziții privind ierarhia și responsabilitatea persoanei responsabile de Politica de securitate

7. Operatorul 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.
8. Politica de securitate a datelor cu caracter personal se va revizui după necesitate, cel puțin o dată în an ca rezultat al modificărilor sau reevaluării competențelor entității. Directorul executiv va desemna persoana/ele care vor elabora nemijlocit ajustarea prevederilor prezentului act.
9. 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.
10. Responsabil de implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, va fi desemnată persoana care conform ordinului Agenției, va dispune de resurse suficiente şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.
11. Persoana responsabilă desemnată, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit directorului executiv al Agenției sau persoanei care îndeplinește interimatul funcției.
12. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.
13. Persoana responsabilă de politica de securitate a datelor cu caracter personal va defini clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală, va asigura măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal, va elabora procedurile de clasificare a informaţiei care conţine date cu caracter personal astfel încît să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date, va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

Secțiunea IV. Mijloacele supuse principiilor de protecție a datelor cu caracter personal

14. Protecţia datelor cu caracter personal în cadrul Agenției este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal.

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

Secţiunea V. Scopul măsurilor de protecţie a datelor cu caracter personal

16. Măsurile de protecţie a datelor cu caracter personal sunt instituite cu scopul:
    1) preîntîmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
    2) preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;
    3) neadmiterea dezvăluirii terţilor a informaţiei cu accesibilitate limitată;
    4) eficientizarea resurselor informaţionale atît pe suport de hîrtie cît şi cel în format electronic.

Secţiunea VI. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale

17. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se realizează prin următoarele metode:
    1) preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
    2) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
    3) preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
    4) preîntîmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
    5) preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea canalelor VPN;
    6) preîntîmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă;
    7) preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent;
    8) stabilirea exactă a ordinii de acces la informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenţă instituite atît pentru utilizatorii interni cît şi pentru cei externi.

Secţiunea VII. Procedurile organizatorice şi tehnice care urmează a fi respectate în cadrul Agenţiei la prelucrarea datelor cu caracter personal

18. Măsurile generale de administrare a securităţii informaţionale sunt:
    1) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.
    2) Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.
    3) Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.

4) Este asigurată securitatea şi accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.
5) Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.
6) Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.
7) Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

19. Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal se realizează prin:
1) Accesul în sediile/oficiile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).
2) Se asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces.
3) Perimetrul de securitate al Agenției reprezintă perimetru oficiilor în care se prelucrează/stochează date cu caracter personal.
4) Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sînt rezistenţi, intrările sunt echipate cu lacăte şi semnalizare.
5) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
6) Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc membrii.
7) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
8) Accesul în perimetrul de securitate a sediului Agenției unde se prelucrează/ stochează date cu caracter personal cu utilaje foto/ video neautorizate este interzis, ţinînd cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 ale Legii nr. 133/2011.
9) 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.

Secțiunea VIII. Identificarea şi autentificarea utilizatorilor

20. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conţine semnalmentele nivelului de accesibilitate al utilizatorului.
21. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.
22. 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 administratorul I.T.
23. Administrarea identificatorilor utilizatorilor va include:
a) identificarea univocă a fiecărui utilizator;
b) verificarea autenticităţii fiecărui utilizator.

Secțiunea IX. Utilizarea parolelor în procesul asigurării securităţii informaţionale, controlul administrării accesului și securitatea electro-energetică

24. Regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor vor include:
a) păstrarea confidenţialităţii parolelor;

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

25. Controlul administrării accesului se va efectua sistematic în privinţa acţiunilor utilizatorilor, în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.
26. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate, supuse monitorizării şi controlului.
27. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este autorizată de persoanele responsabile ale Agenției şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.
28. Accesul fără fir la sistemele informaţionale de date cu caracter personal se limitează la maximum, fiind documentat, supus monitorizării şi controlului.
29. Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.
30. Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale Agenției.
31. Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, se va asigura contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.
32. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, se va asigura posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.
33. Se vor implementa sisteme automatizate de depistare şi de semnalizare a incendiilor în birourile unde sînt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.
34. Se va exercita controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal.
35. Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.

Secțiunea X. Dezvăluirea datelor cu caracter personal

36. Dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidență, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată cu criptarea acestei informații sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidenţă 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, reieşind din posibilităţile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmînarea personală, etc.).
37. Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund Cerinţelor, (spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.) sînt interzise.
38. Sînt interzise operaţiunile de dezvăluire a datelor cu caracter personal între Agenție și alte entități care sunt amplasate geografic în stînga Nistrului care refuză să se supună juridic

legislaţiei Republicii Moldova, reieşind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce ţine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecţia datelor cu caracter personal.

39. Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecţie a datelor cu caracter personal.
40. Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii nr. 133/2011, în special în cazurile cînd tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.
41. Volumul şi categoriile datelor cu caracter personal colectate în scopul ținerii evidenței Agenției, este limitat la strictul necesar pentru realizarea scopurilor declarate.
42. Acces la sistemele informaționale gestionate în cadrul Agenției, din partea Procuraturii Generale (după caz procuraturile teritoriale/specializate), Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi art. 212 Cod de procedură penală. În conformitate cu prevederile art.157 Cod de procedură penală, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adeverite circumstanţe care au importanţă 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 şi răspîndite fără necesitate informaţie oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie 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 instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informaţii o explicaţie în scris care ar confirma necesitatea furnizării datelor menţionate. Se va ţine cont de faptul că în conformitate cu prevederile art.8 al Legii privind accesul la informație, datele cu caracter personal fac parte din categoria informaţiei oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislaţiei privind protecţia datelor cu caracter personal. În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoştinţă cu fişa personală a clientului, aceştia urmează a fi informaţi în scris despre obligaţiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 şi 30 ale Legii privind protecţia datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 741 Cod contravenţional.

Secțiunea XI. Drepturile subiecţilor de date cu caracter personal

43. În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii nr. 133/2011, persoanei necesită a-i fi furnizate următoarele informaţii, exceptînd cazul în care el deţine deja informaţiile respective:
    1) privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidență al operatorilor de date cu caracter personal);
    2) privind scopul concret al prelucrării datelor cu caracter personal colectate;
    3) privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
    4) existenţa drepturilor la informare şi de acces la datele colectate; de intervenţie asupra datelor (în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) şi de opoziţie, 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

consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia.

44. 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.
45. Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entitățile ce asigură mentenața sistemului și sau prestează servicii externalizate ale operatorului) tuturor persoanelor supuse prelucrării.
46. 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 urmînd a fi efectuată în toate sistemele informaţionale și de evidenţă gestionate.

Secțiunea XII. Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate, auditul sistemelor informaționale gestionate

47. Accesul în spaţiile/perimetrul unde sînt amplasate sistemele informaţionale și de evidență a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară conform politicii de securitate instituţionale /regulamentelor departamentale aprobate.
48. Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecţie speciale tehnice şi de program și nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii soft-ului, de asigurare a efectuării periodice a copiilor de siguranţă și de efectuare a auditului - este interzisă.
49. Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredinţate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul Agenției.
50. Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.
51. Auditul sistemelor informaționale gestionate se realizează prin:
    1) înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:
        a) data şi timpul tentativei intrării/ieşirii;
        b) ID-ul utilizatorului;
        c) rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.
    2) înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
        a) data şi timpul tentativei de obţinere a accesului (executate a operaţiunii);
        b) denumirea (identificatorul) aplicaţiei sau procesului, o ID-ul utilizatorului;
        c) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
        d) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
        e) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.

3) înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:
   a) data şi timpul modificării competenţelor;
   b) ID-ul administratorului care a efectuat modificările;
   c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.
4) înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:
   a) data şi timpul eliberării;
   b) denumirea informaţiei şi căile de acces la aceasta;
   c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
   d) ID-ul utilizatorului, care a solicitat informaţia.

Secțiunea XIII. Asigurarea protecției, gestionarea incidentelor de securitate, marcarea documentelor și responsabilitatea asigurării securității datelor

52. Agenția va asigura:
   1) protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existența programelor licențiate anti-virus;
   2) testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).
53. Gestionarea incidentelor de securitate se realizează în următoarele forme:
   1) Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.
   2) Personalul Agenției informează neîntîrziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.
   3) Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.
   4) Pînă la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrul Național pentru Protecția Datelor cu Caracter Personal despre incidentele de securitate constatate.
   5) În cazul producerii incidentelor de securitate în cadrul Agenției, persoana resposabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.
   6) În cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar și asigurat accesul la informațiile necesare relevante obiectului controlului.
54. Toată informația care se intenționează a fi dezvăluită, și care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.
   Model*: Atenţie! Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr. _____, înregistrat în Registrul de evidenţă al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr. 133 /2011 privind protecţia datelor cu caracter personal*
55. Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 741 Cod contravențional) și penală (art. art. 177, 178, 180 Cod penal).

Anexa nr. 2
La Decizia nr. 5 din 14.07.2021

Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă gestionat de către Agenția pentru Dezvoltarea și Modernizarea Agriculturii

Capitolul I. DISPOZIŢII GENERALE

1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal (în continuare Regulament) este elaborat în vederea implementării în cadrul Instituției Publice "Agenția pentru Dezvoltarea și Modernizarea Agriculturii" (în continuare Agenție) - a prevederilor Legii nr.133/2011 privind protecţia datelor cu caracter personal și a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123/2010, precum și întru respectarea prevederilor art. 91 - 94 ale Codului muncii.
2. Regulamentul stabilește condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților Agenției în cadrul sistemului de evidență resurse umane (denumit în continuare "sistemul de evidență").
3. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență constă în asigurarea înregistrării informațiilor referitoare la recrutarea, angajarea, executarea clauzelor contractelor individuale de muncă, pensionarea salariaților, precum și a prezentării rapoartelor trimestriale şi anuale către instituţiile statului, conform legislației în vigoare.
4. În cadrul sistemului de evidență sunt prelucrate următoarele categorii de date cu caracter personal:
   1) numele, prenumele, patronimicul;
   2) sexul;
   3) data și locul nașterii;
   4) semnătura;
   5) date din actele de stare civilă;
   6) Telefon mobil;
   7) E-mail;
   8) Profesie, funcție;
   9) Formare profesională;
   10) Situația familială;
   11) Situație economică și financiară;
   12) Datele membrilor de familie;
   13) Cetățenia;
   14) Sancțiuni disciplinare;
   15) CPAS;
   16) Adresa (domiciliu/reședința);
   17) Loc de muncă;
   18) IDNP;
   19) Date bancare;
   20) Imagine: cetățenia, IDNP;
   21) mărime salariu brut, prime, stimulări, sporuri, suplimente, date din certificatul de concediu medical;
   22) după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.
5. Prelucrarea datelor cu caracter personal menționate în cadrul sistemului de evidență resurse umane va fi efectuată pentru realizarea următoarelor scopuri:
   1) Realizării activităților aferente recrutării;
   2) Încheierea și executarea contractelor de muncă;
   3) Furnizarea de beneficii;
   4) Prezentarea la CNAM a evidenţei nominale a noilor angajaţi şi a celor concediaţi, format electronic;
   5) Administrarea resurselor umane la nivelul Agenției (de ex., evaluare, training, proceduri disciplinare, plata salariilor, registre de personal, asigurarea securității și sănătății în muncă);

6) Desfășurarea de controale interne și externe de tip audit, cat si pentru cooperarea cu organizatiile profesionale;
7) Arhivare, îndeplinirea obligațiilor legale, apărare în caz de litigiu sau orice formă de neînțelegere între salariat și Agenție.

6. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către astfel încît să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămîne la păstrare primind statut de document de arhivă.

Capitolul III. LOCAȚIA ȘI DESCRIEREA SISTEMUL DE EVIDENȚĂ RESURSE UMANE

7. Datele cu caracter personal conținute în sistemul de evidență în cadrul Agenției se prelucrează/stochează pe suport de hîrtie.
8. Prelucrarea informațiilor în sistemul de evidență pe suport de hîrtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri, care sînt amplasate fizic în biroul 3 etajul 3 din sediul, mun. Chișinău, str. Calea Basarabiei, 18, MD-2023.

Capitolul IV. DURATA DE STOCARE

9. Prelucrarea datelor cu caracter personal în sistemul de evidență resurse umane se efectuează pe perioada activității angajaților Agenției, valabilității contractelor individuale de muncă (din momentul semnării contractului până la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).
10. Datele cu caracter personal a potențialilor salariați se preia din CV-ul transmis de către aceștia la adresa de e-mail a Agenției. După primirea CV-ului prin intermediul poștei electronice, acesta se tipărește pe suport de hârtie, iar de pe adresa de e-mail se șterge conținutul mesajului. Totodată, în cazul în care potențialii salariați nu au fost admiși la funcția vacantă din cadrul Agenției, atunci persoana responsabilă de sistemul de evidență a resurselor umane distruge CV-urile potențialilor angajați.
11. La expirarea termenelor menționate în pct. 9, datele din sistemul de evidență resurse umane sînt păstrate în formă arhivată, pe perioada stabilită de Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova, aprobat de Agenția Națională a Arhivelor nr.57/2016, ulterior fiind supuse distrugerii sau ștergerii, în funcție de suportul pe care au fost efectuate.

Capitolul V. DREPTURILE PERSOANELOR VIZATE

12. Agenția în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.
13. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.
14. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență vor respecta procedura de acces la datele cu caracter personal.
15. Acordarea dreptului de acces a persoanelor vizate la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al directorului Agenției. Informațiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.
16. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informaţiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.
17. Prelucrarea datelor cu caracter personal ale potențialilor salariați, precum și a salariaților se efectuează în conformitate cu art. 5 alin. (5) lit. a) și lit. b) ale Legii nr. 133/2011, și anume: în cazul executării unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea

unor măsuri înaintea încheierii contractului, la cererea acestuia (în cazul încheierii contractului indivual de muncă) şi în cazul îndeplinirii unei obligaţii care îi revine operatorului conform legii (în conformitate cu legislaţia muncii).

Capitolul VI. MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENŢĂ RESURSE UMANE

18. Măsurile generale de administrare a securităţii informaţionale sunt:
    1) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie care conţin date preluate din sistemul de evidenţă, aceştia se păstrează în safeuri care se încuie.
    2) La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la reţeaua electrică.
    3) Operatorul asigură securitatea punctelor de primire şi expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.
    4) Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidenţă este blocat împotriva vizualizării de către persoane neautorizate.
    5) Mijloacele de prelucrare a informaţiilor preluate din sistemul de evidenţă sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
19. Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidenţă din/în perimetrul de securitate se înregistrează în registru.
20. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidenţă, se înfăptuiesc ţinînd cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală.
21. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă, care conţin date cu caracter personal, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal. Model Atenţie! Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr. _____, înregistrat în Registrul de evidenţă al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal.
22. Accesul în birourile ADMA este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program.
23. Biroul nu este lăsat niciodată fără supraveghere la ieşirea în exterior.
24. Înainte de acordarea accesului fizic la sistemul de evidenţă, se verifică competenţele de acces.
25. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.
26. Perimetrul de securitate se consideră perimetrul birourilor în care este amplasat sistemul de evidenţă, fiind integre din punct de vedere fizic.
27. Zilnic, se inspectează perimetrele de securitate al clădirii şi al biroului, din punct de vedere fizic.
28. Accesul persoanelor neautorizate în cadrul perimetrelor de securitate va fi chestionat pentru a evita accesul neautorizat şi fiecare situaţie va fi raportată persoanelor responsabile cu acordarea drepturilor de acces şi asigurarea securităţii.
29. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.
30. Amplasarea sistemului de evidenţă răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
31. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă , a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemul de evidenţă, inclusiv posibilitatea deconectării oricărui component TI.
32. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaţionale.
33. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul

sistemului de evidență. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

Capitolul VII. AUDITUL SECURITĂŢII ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE

34. Se organizează generarea înregistrărilor de audit a securităţii în sistemul de evidență pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.
35. Înregistrările de audit a securităţii sistemului de evidență în care sînt prelucrate date cu caracter personal, trebuie să conţină:
    1) numele şi prenumele utilizatorului;
    2) numele fişei accesate (pagina şi inscripţia din registru);
    3) numărul înregistrărilor efectuate;
    4) tipul de acces;
    5) data accesului (an, lună, zi);
    6) timpul (ora, minuta) şi durata accesului.
36. Rezultatele auditului securităţii în sistemul de evidență (operaţiunile de prelucrare a informațiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.
37. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidență constituie 2 /doi/ ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

Capitolul VIII. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ RESURSE UMANE

38. Persoanele care asigură exploatarea sistemului de evidență trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.
39. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidență.
40. În cazul producerii incidentelor de securitate persoanele responsabile vor întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar și să asigure accesul la informațiile necesare relevante obiectului controlului.
41. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informațiilor din sistemul de evidență poartă răspundere civilă, contravențională și penală.

Capitolul IX. Specificul legislației muncii privind prelucrarea datelor personale ale salariaților

42. În conformitate cu art. 91 al Codului Muncii, angajatorul şi reprezentanţii lui sunt obligaţi să respecte următoarele cerinţe:
    a) prelucrarea datelor personale ale salariatului poate fi efectuată exclusiv în scopul îndeplinirii prevederilor legislaţiei în vigoare, acordării de asistenţă la angajare, instruirii şi avansării în serviciu, asigurării securităţii personale a salariatului, controlului volumului şi calităţii lucrului îndeplinit şi asigurării integrităţii bunurilor unităţii;
    b) la determinarea volumului şi conţinutului datelor personale ale salariatului ce urmează a fi prelucrate, angajatorul este obligat să se conducă de legislaţia în vigoare;
    c) toate datele personale urmează a fi preluate de la salariat sau din sursa indicată de acesta;
    d) angajatorul nu este în drept să obţină şi să prelucreze date referitoare la convingerile politice şi religioase ale salariatului, precum şi la viaţa privată a acestuia. În cazurile prevăzute de lege, angajatorul poate cere şi prelucra date despre viaţa privată a salariatului numai cu acordul scris al acestuia;

e) angajatorul nu este în drept să obţină şi să prelucreze date privind apartenenţa salariatului la sindicate, asociaţii obşteşti şi religioase, partide şi alte organizaţii social-politice, cu excepţia cazurilor prevăzute de lege;
f) la adoptarea unei decizii care afectează interesele salariatului, angajatorul nu este în drept să se bazeze pe datele personale ale salariatului obţinute exclusiv în urma prelucrării automatizate sau pe cale electronică;
g) protecţia datelor personale ale salariatului contra utilizării ilegale sau pierderii este asigurată din contul angajatorului;
h) salariaţii şi reprezentanţii lor trebuie să fie familiarizaţi, sub semnătură, cu documentele vizând modul de prelucrare şi păstrare a datelor personale ale salariaţilor din unitate şi să fie informaţi despre drepturile şi obligaţiile lor în domeniul respectiv;
i) salariaţii nu trebuie să renunţe la drepturile lor privind păstrarea şi protecţia datelor personale;
j) angajatorii, salariaţii şi reprezentanţii lor trebuie să elaboreze în comun măsurile de protecţie a datelor personale ale salariaţilor.

43. Conform art. 92 al CM, la transmiterea datelor personale ale salariatului, angajatorul trebuie să respecte următoarele cerinţe:
a) să nu comunice unor terţi datele personale ale salariatului fără acordul scris al acestuia, cu excepţia cazurilor când acest lucru este necesar în scopul prevenirii unui pericol pentru viaţa sau sănătatea salariatului, precum şi a cazurilor prevăzute de lege;
b) să nu comunice datele personale ale salariatului în scopuri comerciale fără acordul scris al acestuia;
c) să prevină persoanele care primesc datele personale ale salariatului despre faptul că acestea pot fi utilizate doar în scopurile pentru care au fost comunicate şi să ceară persoanelor în cauză confirmarea în scris a respectării acestei reguli. Persoanele care primesc datele personale ale salariatului sunt obligate să respecte regimul de confidenţialitate, cu excepţia cazurilor prevăzute lege;
d) să permită accesul la datele personale ale salariatului doar persoanelor împuternicite în acest sens, care, la rândul lor, au dreptul să solicite numai datele personale necesare exercitării unor atribuţii concrete;
e) nu solicite informaţii privind starea sănătăţii salariatului, cu excepţia datelor ce vizează capacitatea salariatului de a-şi îndeplini obligaţiile de muncă;
f) să transmită reprezentanţilor salariaţilor datele personale ale salariatului în modul prevăzut de prezentul cod şi să limiteze această informaţie numai la acele date personale care sunt necesare exercitării de către reprezentanţii respectivi a atribuţiilor lor.

44. Conform art. 93 al CM, în scopul asigurării protecţiei datelor sale personale care se păstrează la angajator, salariatul are dreptul:
a) de a primi informaţia deplină despre datele sale personale şi modul de prelucrare a acestora;
b) de a avea acces liber şi gratuit la datele sale personale, inclusiv dreptul la copie de pe orice act juridic care conţine datele sale personale, cu excepţia cazurilor prevăzute de legislaţia în vigoare;
c) de a-şi desemna reprezentanţii pentru protecţia datelor sale personale;
d) de a avea acces la informaţia cu caracter medical ce-l vizează, inclusiv prin intermediul lucrătorului medical, la alegerea sa;
e) de a cere excluderea sau rectificarea datelor personale incorecte şi/sau incomplete, precum şi a datelor prelucrate cu încălcarea cerinţelor prezentului cod. În cazul în care angajatorul refuză să excludă sau să rectifice datele personale incorecte, salariatul este în drept să notifice în scris angajatorului dezacordul său motivat;
f) de a ataca în instanţa de judecată orice acţiuni sau inacţiuni ilegale ale angajatorului admise la obţinerea, păstrarea, prelucrarea şi protecţia datelor personale ale salariatului.

Capitolul X. DISPOZIŢII FINALE

45. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea Agenția periodic, însă cel puțin o dată în an, precum și la necesitate.
46. Prezentul Regulament se completează cu prevederile legislației în vigoare.
47. Regulamentul este adus la cunoştinţa angajaților prin comunicare directă sau prin publicarea pe pagina de Internet ale Agenția.
48. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.