POLITICA DE SECURITATE PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR INFORMAŢIONALE GESTIONATE DE SOCIETATEA CU RĂSPUNDERE LIMITATĂ ”IQVIN-SERVICE”

2019

SUMAR:

1. PREAMBUL

Societatea cu Răspundere Limitată ”IQVIN-SERVICE” asigură protecţia drepturilor şi libertăţilor fundamentale ale persoanei fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieţii intime, familiale şi private.

Prezenta Politică de Securitate reprezintă un document 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.

Prelucrarea datelor cu caracter personal în cadrul entităţii are loc în baza principiilor prevăzute de actele **internaţionale în domeniu, cît şi de actele normative naţionale în vigoare**:

a) Declaraţia universală a drepturilor omului**;**
b) Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale;
c) Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal;
d) Directiva 95/46/CE a Parlamentului European şi a Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
e) Protocolul adiţional la Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, cu privire la autorităţile de supraveghere şi fluxul transfrontalier al datelor, semnat la 29 aprilie 2010 şi ratificat la 24 iunie 2011;
f) Constituţia Republicii Moldova,
g) Legea privind protecţia datelor cu caracter personal,
h) Legea privind accesul la informaţie,
i) 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 din 14 decembrie 2010,
j) Regulamentului Registrului de evidenţă al operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr. 296 din 15 mai 2012 şi alte acte legislative/normative de profil.

Dreptul la inviolabilitatea vieţii private este este reglementat şi de alte acte normative internaţionale în domeniul drepturilor omului:

a) art. 17 din Pactul internaţional cu privire la drepturile civile şi politice (ratificat prin Hot. Parl. nr.217-XII din 28.07.90 şi în vigoare pentru Republica Moldova din 26 aprilie 1993);
b) art. 12 din Declaraţia universală a drepturilor omului (Republica Moldova a aderat la Declaraţie prin Hot. Parl. nr.217-XII din 28.07.90);
c) art. 8 din Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale (Adoptată la Roma la 04 noiembrie 1950 de către statele membre ale Consiliului Europei; intrată în vigoare la 03 septembrie 1953; ratificată prin Hot. Parl. nr.1298-XIII din 24.07.97 şi în vigoare pentru Republica Moldova din 12 septembrie 1997).

2. INTRODUCERE

Societatea cu Răspundere Limitată "IQVIN-COLECT", ulterior modifictă denumirea în SRL "IQVIN-SERVICE" cu adresa juridică : or. Soroca, str. Alexandru cel Bun 16, şi operează în baza legilor din Republica Moldova, fiind înregistrată de Camera Înregistrarii de Stat a Republicii Moldova şi inclusă în Registrul de Stat al persoanelor juridice din Republica Moldova sub IDNO 1015607001225 la data de 15.06.2015.

Prezenta Politică este aprobată în vederea conformării Societăţii cu Răspundere Limitată "IQVIN-SERVICE" cu prevederile *Hotărârii Guvernului Republicii Moldova nr.1123 din data de 14 decembrie 2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal* precum şi cu *Legea Republicii Moldova nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal*.

3. NOŢIUNI GENERALE

Prezenta Politică de Securitate, utilizează următoarele noţiuni:

a) ***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;
b) ***autentificare –*** procesul de verificare a identificatorului atribuit subiectului de acces;
c) ***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;
d) ***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;
e) ***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.
f) ***fişiere temporare –*** ansamblu de date stocate pe un suport digital, create pentru o perioadă determinată de timp;
g) ***identificare*** - atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;
h) ***integritate*** - certitudinea, necontradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;

i) *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;

j) *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;

k) *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;

l) *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;

m) *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;

n) *politica de securitate a datelor cu caracter personal* **-** document, elaborat de către operatorul de date cu caracter personal Societatea cu Răspundere Limitată "IQVIN-SERVICE", 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;

o) *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;

p) *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;

q) *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;

r) *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;

s) *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;

t) *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;

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

w) *tehnologie informaţională ((TI) eng. - informational technologic)* – totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

x) *control de securitate* – acţiuni întreprinse de către Societatea cu Răspundere Limitată ”IQVIN-SERVICE” în vederea verificării şi/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute manual;

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

4. SCOPUL IMPLIMENTĂRII POLITICII DE SECURITATE

Acest document reprezintă şi confirmă în acelaşi timp, angajamentul şi responsabilitatea Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”, pentru asigurarea unui nivel suficient de înalt al securităţii informaţionale şi nemijlocit al protecţiei datelor cu caracter personal prelucrate.

Scopul şi obiectivele principale ale Politicii de securitate sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de Societatea cu Răspundere Limitată ”IQVIN-SERVICE”, atît în cadrul prelucrării manuale, cît şi în cadrul sistemelor şi proceselor de tehnologie informaţională.

Integritatea face trimitere la toate măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate a acestora.

Prin **disponibilitate** se înţelege asigurarea funcţionării continue a tuturor componentelor sistemului informaţional.

Confidenţialitatea asigură protecţia datelor împotriva accesului neautorizat.

Securitatea informaţională reprezintă o componentă esenţială a derulării optime a proceselor bazate pe tehnologii informaţionale în cadrul Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”.

Implimentarea unei securităţi informaţionale adecvate este asigurată prin respectarea prezentei Politici de către angajaţii Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”.

Politica dată cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datelor cu caracter personal, sistemelor şi proceselor informaţionale, 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 legislaţiei.

Rolul Politicii de securitate este de a-i informa pe angajaţii Societăţii cu Răspundere Limitată ”IQVIN-SERVICE” asupra modului în care aceştia trebuie să se comporte în ceea ce priveşte situaţiile de lucru cu informaţii care deţin date cu caracter personal, precum şi acţiunile specifice pe care angajaţii urmează să le întreprindă în funcţie de situaţiile apărute. În acest sens, angajaţii Societăţii cu Răspundere Limitată ”IQVIN-SERVICE” urmează să respecte strict prevederile Politicii de securitate şi regulile interne ale Societăţii cu Răspundere Limitată ”IQVIN-SERVICE” privind protecţia datelor cu caracter personal şi sistemelor informaţionale.

5. IMPLIMENTAREA POLITICII DE SECURITATE

Prezenta Politică de securitate se revizuieşte cel puţin o dată în an, ca rezultat al modificărilor sau reevaluării componentelor acestuia şi este aprobat de Administratorul Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”.

Politica de securitate, în mod obligatoriu va fi adusă la cunoştinţă, sub semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

Pentru implimentarea prezentei politici va fi desemnată o Persoană responsabilă de politica de securitate a datelor cu caracter personal, care va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceastea nu operează în afara cadrului acestei politici, totodată va avea diferite responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

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

1. RESURELE INFORMAŢIONALE SUPUSE PROTECŢIEI

În cadrul Societăţii cu Răspundere Limitată ”IQVIN-SERVICE” sunt supuse protecţiei toate resursele informaţionale, care conţin date cu caracter personal, inclusiv:

a) suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;
b) sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi multiplicare a documentelor, alte mijloace tehnice de prelucrare a informaţiei.

2. SCOPUL APLICĂRII MĂSURILOR DE PROTECŢIE A DATELOR CU CARACTER PERSONAL :
   a) preîntîmpinarea scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la datele cu caracter personal;
   b) preîntîmpinarea distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;
   c) respectarea cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;
   d) asigurărea caracterului complet, integru şi veridic al datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;
   e) păstrarea posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.

3. METODELE EFECUĂRII PROTECŢIEI DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAŢIONALE :
   a) preîntîmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
   b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
   c) preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
   d) preîntîmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor angajaţi ai deţinătorului de date cu caracter personal, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program.
   e) preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canale de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea protocolului de transfer SFTP.
   f) 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.
   g) separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a sistemelor informaţionale, prin izolarea funcţiilor de securitate de funcţiile care nu se atribuie la securitatea acestui sistem şi posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităţilor, a folosirii resurselor informaţionale în care sînt prelucrate date cu caracter personal.
   h) monitorizarea permanentă şi controlul comunicaţiilor la perimetrul exterior al sistemelor informaţionale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaţionale.
   i) este asigurată imposibilitatea accesului din exterior a utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal, totodată asigurîndu-se integritatea şi confidenţialitatea datelor cu caracter personal transmise prin utilizarea mijloacelor de protecţie criptografică a informaţiei şi semnătura digitală.

4. SECURITATEA MEDIULUI FIZIC ŞI A TEHNOLOGIILOR INFORMAȚIONALE FOLOSITE ÎN PRELUCRAREA DATELOR CU CARACTER PERSONAL
   a) Accesul în biroul unde sunt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare - insigne, ecusoane, cartele de identificare.
   b) Se efectuează administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces şi competenţele de acces.
   c) Perimetrul de securitate al Societăţii cu Răspundere Limitată ”IQVIN-SERVICE” reprezintă perimetrul oficiului în care se prelucrează/stochează date cu caracter personal.
   d) Perimetrul încăperii în care se prelucrează/stochează date cu caracter personal este integru din punct de vedere fizic, pereţii exteriori sunt rezistenţi, iar intrarea este echipată cu lacăte.
   e) Societaţea cu Răspundere Limitată ”IQVIN-SERVICE” dispune de safeu metalic şi dulapuri care se incuie la cheie.
   f) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
   g) 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.
   h) Uşile se încuie în cazul în care în încăpere lipsesc angajaţii Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”.
   i) Agendele şi/sau cărţile de telefoane în care se conţin indicii despre locul amplasării mijloacelor de prelucrare a datelor cu caracter personal nu sunt accesibile persoanelor străine.
   j) Purtătorii de informaţii şi mijloacele de prelucrare a datelor cu caracter personal scoase din încăperile aflate în perimetrul de securitate nu vor fi lăsate fără supraveghere în locuri publice.
   k) Intrarea în imobilul în care îsi are oficiul Societatea cu Răspundere Limitată ”IQVIN-SERVICE”, este păzit de ÎS „Pază de Stat”.

5. MĂSURILE GENERALE DE ADMINISTRARE A SECURITĂŢII INFORMAȚIONALE
   a) 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.
   b) Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.
   c) Computerele Societăţii cu Răspundere Limitată ”IQVIN-SERVICE” sunt dotate cu parolă de acces pentru intrarea în sistem, întru prevenirea accesului neautorizat a terţelor persoane, iar în cazul nefolosirii computerului mai mult de 15 minute el se blochează.
   d) Se asigură securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele scanare şi de copiere.
   e) Se asigură securitatea şi se împiedică accesul fizic al persoanelor neautorizate la informaţia care conţine date cu caracter personal.
   f) Orice instalare a soft-urilor de gen *shareware* sau *freeware* este permisă numai cu acordul Administratorului Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”.

g) 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 Administratorului Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”.

7. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

1. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI

a) În sistemele informaţionale care conţin date cu caracter personal, este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.
b) Toţi utilizatorii au un identificator unic (ID-ul utilizatorului).
c) Pentru a confirma ID-ul, utilizatorul utilizează parole.
d) În cazul în care contractul de muncă ale utilizatorului au fost încetate, suspendate sau modificate, iar noile sarcini nu necesită accesul la date cu caracter personal, accesul la informaţia cu caracter personal se suspendă.
e) Dacă utilizatorul a abuzat de codurile primite, şi implicit, de informaţia cu caracter personal, în scopul comiterii unei fapte prejudiciabile, ori a absentat o perioadă îndelungată, codurile de identificare şi autentificare după caz se revocă sau se suspendă.

2. IDENTIFICAREA ŞI AUTENTIFICAREA ECHIPAMENTULUI

a) În cazul accesului la informaţia cu caracter personal, se asigură posibilitatea identificării, autentificării şi accesului la echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal, cu menţinerea acestor informaţii pentru o perioadă îndelungată.

3. ADMINISTRAREA IDENTIFICATORILOR UTILIZATORILOR

a) Verificarea autenticității fiecărui utilizator
a) Identitatea univocă a fiecărui utilizator

4. UTILIZAREA ŞI ADMINISTRAREA PAROLELOR

Accesul la echipamentul care operează cu date personale, se asigură prin folosirea unei parole care previne accesul neautorizat la astfel de informaţii. Administrarea şi asigurarea parolelor prevede un şir de măsuri tehnice, care includ:

a) confidenţialitatea parolei;
b) prevenirea şi interzicerea memorării parolei pe suport de hîrtie sau digital, în cazul în care nu se asigură securitatea păstrării acestuia;
c) modificarea parolei atunci cînd există temeiuri pentru o eventuală compromitere a acesteia;
d) alegerea parolelor calitative care să conţină minimum 8 simboluri, acestea fiind diferite una de alta, şi nu sînt compuse integral din grupuri de cifre sau litere;
e) modificarea parolelor după necesitate, dar nu mai puţin de o dată la 3 luni;
f) dezactivarea procesului automatizat de completare şi salvare a parolelor. (cu folosirea parolelor salvate)
g) se folosesc idenficatoare individuale pentru fiecare utilizator şi parole individuale ale acestora pentru asigurarea posibilităţii de stabilire a responsabilităţii.

h) Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora.

8. CONTROLUL ADMINISTRĂRII ACCESULUI

a) Acţiunile utilizatorilor sînt controlate sistematic de către conducătorul unităţii în vederea analizei şi evaluării corectitudinii, conformării şi acţiunilor efectuate în cadrul sistemelor informaţionale de date cu caracter personal.

9. BLOCAREA SESIUNII DE LUCRU

a) Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal, se blochează la solicitarea utilizatorului sau automat, după 15 minute de perioadă inactivă a utilizatorului, fapt care face imposibil accesul de mai departe pînă în momentul cînd utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

10. MARCAREA DOCUMENTELOR

a) Toată informaţia care urmează a fi dezvăluită, şi care conţine date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidenţă al operatorilor de date cu caracter personal precum şi se indică prescripţii pentru prelucrarea şi răspîndirea ulterioară a acesteia.
Model: Acest document conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr.0000, înregistrat în Registrul de evidenţă al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată doar în condiţiile prevăzute de Legea privind protecţia datelor cu caracter personal.

11. ACCESUL DE LA DISTANŢĂ

a) Toate metodele prin care se efectuează accesul de la distanţă la informaţia cu caracter personal sînt securizate în mod obligatoriu, utilizîndu-se în acest sens criptarea, cifrarea informaţiilor, etc. Fiecare acces la distanţă este monitorizat, controlat şi documentat.
b) Accesul la distanţă la sistemul informaţional este autorizat de către persoana responsabilă, fiind permisă doar în măsura în care informaţia prin accesul la distanţă le este necesară pentru îndeplinirea obiectivelor stabilite.

12. LIMITAREA FOLOSIRII TEHNOLOGIEI FĂRĂ FIR

a) Accesul fără fir la sistemele informaţionale de date cu caracter personal se limitează, fiind documentat, monitorizat şi controlat de către administratorul Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”.
b) În cazul accesului fără fir la sistemele informaţionale de date cu caracter personal, se utilizează mijloace de criptare a informaţiei.
c) Folosirea tehnologiilor fără fir se autorizează de către conducătorul Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”.

13. CONTROLUL INSTALĂRII ŞI SCOATERII COMPONENTELOR TI

a) Informaţiile, care conţin date cu caracter personal şi care se află pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.
b) Este exercitat 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.

14. SECURITATEA CABLURILOR DE REȚEA

a) Cablurile de reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, sunt protejate contra conectărilor nesancţionate sau deteriorării
b) Cablurile de tensiune sunt separate de cele comunicaţionale pentru excluderea bruiajului.
c) Administratorul Societăţii cu Răspundere Limitată ”IQVIN-SERVICE”, efectuează controale, nu mai rar decît o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea.

15. SECURITATEA ELECTROENERGETICĂ

a) Echipamentul electric utilizat pentru buna funcţionare a sistemelor informaţionale de date cu caracter personal, este asigurat împotriva unor deteriorări şi conectări ilegale, prin montarea lor în nişe speciale.
b) În cazul apariţiei situaţiilor de forţă majoră, se asigură asigurată posibilitatea deconectării electricităţii de la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectărilor oricărui component TI.
c) Sunt instale surse autonome de alimentare cu energie electrică (Back-UPS), care sunt folosite pentru terminarea corectă a sesiunii de lucru şi a sistemului (componentului) în cazul deconcetării de la sursa principală de alimentare cu energie electrică.

16. ASIGURAREA PROTECȚIEI CONTRA PROGRAMELOR DĂUNĂTOARE (VIRUȘILOR)

a) Este asigurată protecţia contra infiltrării programelor dăunătoare în softu-rilor destinate prelucrării datelor cu caracter personal, prin instalarea programelor de anti-virus.

17. TESTAREA POSIBILITĂȚILOR FUNCȚIONALE DE ASIGURARE A SECURITĂȚII SISTEMELOR INFORMAȚIONALE DE DATE CU CARACTER PERSONAL

a) Se asigură 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).

18. COPIILE DE REZERVĂ ALE INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL

a) Regulat, dar nu mai rar de o data la jumatate de an, persoana responsabilă va efectua copia de rezervă a informaţie ce conţine date cu caracter personal.

19. STOCAREA ŞI PĂSTRAREA DATELOR CU CARACTER PERSONAL PRELUCRATE

a) Este interzisă stocarea şi păstrarea formatului electronic al datelor cu caracter personal, în computere care sînt conectate la internet şi nu sînt echipate cu mijloace de protecţie nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii soft-ului, de asigurare a efectuării periodice a copiilor de siguranţă şi de efectuare a auditului.

b) Se interzice utilizarea calculatoarelor personale şi purtătorilor de informaţii în scop de serviciu.

c) 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 dulapuri de lemn care se încuie, safeuri de fier sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

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

a) Înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, se efectuează conform următorilor parametri:

- data şi timpul tentativei intrării/ieşirii;
- ID-ul utilizatorului
- rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.

b) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- data şi timpul tentativei de obţinere a accesului (executate a operaţiunii),
- denumirea (identificatorul) aplicaţiei sau procesului, o ID-ul utilizatorului,
- specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.),
- tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.),
- rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.

c) Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

- data şi timpul modificării competenţelor,
- ID-ul administratorului care a efectuat modificările,
- ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

d) Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

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

21. GESTIONAREA INCIDENTELOR DE SECURITATE

a) 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.
b) Angajaţii Societăţii cu Răspundere Limitată "IQVIN-SERVICE" informează neîntîrziat conducerea despre incidentele care încalcă securitatea datelor cu caracter personal.
c) Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.
d) Pînă la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează Centrul pentru protecţia datelor cu caracter personal despre incidentele de securitate constatate.
e) Persoanele împuternicite de către operator şi alte persoane vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia datelor personale poartă răspundere disciplinară, materială, contravenţională şi penală în modul prevăzut de legislaţia în vigoare.

22. DISPOZIŢII FINALE

a) Modificarea şi completarea prezentei Politici se face în modul stabilit pentru aprobarea ei.