REPUBLICA MOLDOVA
Raionul Făleşti
Consiliul comunal Sărata Veche
MD-5947
Tel.(259)-64-336, (259)-64-338

РЕСПУБЛИКА МОЛДОВА
Фэлештский Район
Комунальный совет Сэрата Веке
MD-5947
Тел.(259)-64-336, (259)-64-338

DECIZIE nr.8/1
din 22.12.2021

Cu privire la aprobarea politicii
de securitate a datelor cu caracter
personal

În temeiul art.14 (1) al Legii, privind administraţia publică locală nr.436-XVI din 28.12.2006, art. 4 (3) al Legii privind descentralizarea administrativă nr. 435 din 28.12.2006, Legii nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal, Hotărârii Guvernului Republicii Moldova nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, Consiliul comunal Sărata Veche

DECIDE:

1. Se aprobă politica de securitate a datelor cu caracter personal conform anexei nr. 1.
2. Responsabil pentru executarea prezentei decizii este primarul comunei Sărata Veche dna Galiț Maria.

Preşedintele şedinţei Paladi Varvara

Secretarul Consiliului Caras Ghenadie

Anexa nr. 1 la
Decizia nr.8/1 din 22.12.2021

POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

1. Scopul Politicii de securitate a datelor cu caracter personal

Prezenta Politică de securitate a datelor cu caracter personal (denumită în continuare „**Politica**") descrie condițiile și modul de desfășurare a activității de prelucrare a datelor cu caracter personal ale subiecților datelor cu caracter personal, precum și a măsurilor de securitate și trăsăturile de protecție selectate pentru securitatea datelor.

Măsurile de protecția datelor cu caracter personal sunt asigurate în scopul:

- preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețele de telecomunicații și resursele informaționale;
- neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- eficientizarea resurselor informaționale atât pe suport de hârtie cât și cel în format electronic.

Prezenta Politică este aprobată, inclusiv, în vederea conformării Primăriei comunei Sărata Veche cu prevederile Hotărârii Guvernului Republicii Moldova nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal și Legii Republicii Moldova nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

2. Domeniul de aplicare al Politicii

2.1 Politica reglementează modul în care sunt colectate și prelucrate datele personale, precum și condițiile de utilizare a informației respective în cadrul Pimăriei comunei Sărata Veche, operator de date cu caracter personal, persoană juridică înregistrată în Republica Moldova, având sediul la MD-5946, str. Independenței, nr. 6, s. Sărata Veche, rl Fălești, Republica Moldova, IDNO 1007601002692 (denumită în continuare „**Compania**").

2.2 Politica se aplică datelor personale ale subiecților datelor cu caracter personal (date înregistrate pe suport de hârtie și/sau în format electronic) prelucrate și deținute de către Companie.

2.3 Obiectivele principale ale Politicii sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv a datelor cu caracter personal prelucrate de Companie, atât în cadrul prelucrării manuale, cât și în cadrul sistemelor și proceselor de tehnologie informațională (denumită în continuare „**IT**").

Securitatea este o componentă esențială a derulării optime a proceselor bazate pe tehnologiile informaționale în cadrul Companiei. Politica cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv datelor cu caracter personal, sistemelor și proceselor bazate pe tehnologiile informaționale împotriva influențelor naturale, erorilor umane și tehnice, precum și împotriva acțiunilor deliberate care pot provoca pagube materiale, imateriale, sau care pot duce la încălcări ale legislației. Având în vedere că siguranța IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic și de altă natură.

Compania va proteja datele cu caracter personal a angajaților săi, a angajaților clienților săi, dar și a altor persoane fizice, prelucrate de către Companie.

Reglementările prezentei Politici reprezintă un standard minim pentru Companie, inclusiv toți angajații acesteia. Pornind de la această reglementare, toți angajații urmează să respecte strict

prevederile Politicii şi regulile interne ale Companiei privind protecţia datelor cu caracter personal şi sistemelor IT.
2.4 În Politică sunt utilizate următoarele noţiuni:
a. date cu caracter personal – orice informaţii referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulţi factori specifici identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;
b. autentificare – verificarea identificatorului atribuit subiectului de acces şi confirmarea autenticităţii;
c. prelucrarea datelor cu caracter personal – orice operaţiune sau set 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 către terţi prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;
d. control de securitate - acţiuni întreprinse de către Companie în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute;
e. identificare - atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;
f. integritate - certitudinea, ne-contradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;
g. 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;
h. 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;
i. perimetru de securitate - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic şi/sau tehnic al accesului;
j. 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;
k. purtător de date cu caracter personal - suport magnetic, optic, laser, de hârtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia;
l. 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;
m. sesiune de lucru - perioada care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale şi până la momentul opririi acestora;
n. stocarea – păstrarea, pe orice fel de suport, a datelor cu caracter personal;
o. sistem de evidenţă a datelor cu caracter personal – orice serie structurată de date cu caracter personal, accesibilă potrivit unor criterii determinate, indiferent dacă această structură este organizată în mod centralizat ori descentralizat sau este repartizată după criterii funcţionale ori geografice;

p. utilizator – orice persoană care acționează sub autoritatea Companiei, respectiv a reprezentantului său permanent, cu drept recunoscut de acces la bazele de date cu caracter personal;
q. sistem informațional - totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal.

3. Documente de referință
a. Declarația universală a drepturilor omului, a Națiunilor Unite din 10.12.1948;
b. Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, a Consiliului Europei din 04.11.1950;
c. Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, semnată la Strasbourg la 28.01.1981 și ratificată de Republica Moldova prin Hotărârea Parlamentului nr. 483 din 02.07.1999;
d. Constituția Republicii Moldova;
e. Legea privind protecția datelor cu caracter personal nr. 133 din 08.07.2011;
f. Legea privind accesul la informație nr. 982 din 11.05.2000;
g. Legea cu privire la registre nr. 71 din 22.03.2007;
h. Hotărârea Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
i. Hotărârea Guvernului nr. 296 din 15.05.2012 privind aprobarea Regulamentului registrului de evidență al operatorilor de date cu caracter personal.

4. Responsabilități
Principala responsabilitate în elaborarea, implementarea și monitorizarea aplicării prevederilor prezentei Politici revine persoanei responsabile a Companiei care va fi numită printr-un ordin intern. Persoana responsabilă se subordonează nemijlocit conducătorului (administratorului) Companiei și nu va avea responsabilități incompatibile cu sarcinile funcției de implementare a prezentei Politici.
Modificarea persoanei responsabile de implementarea și monitorizarea respectării prevederilor prezentei Politici, va fi făcută prin desemnarea persoanei conform fișei postului și/sau ordinului intern.
Persoana responsabilă nou desemnată, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor Politicii, se va subordona nemijlocit conducătorului (administratorului) Companiei sau persoanei care îndeplinește interimatul funcției.
Compania va pune la dispoziția persoanei responsabile de implementarea prezentei Politici resurse suficiente (timp, resurse umane, echipament și buget) și ii va oferi acces liber la informația necesară pentru îndeplinirea funcțiilor sale, în măsura în care aceasta nu operează în afara cadrului acestei Politici.
Persoana responsabilă de prezenta Politică asigură definirea clară a diferitelor responsabilități cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare și prelucrare), precum și operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau a altor împrejurări. Persoana responsabilă de prezenta Politică va defini clar responsabilitățile și procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională și de funcționare generală, va asigura măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal.

5. Descrierea procedurilor (organizatorice și tehnice) de prelucrare și de securitate

Prezenta Politică, aplicabilă la nivelul Companiei, reglementează măsurile tehnice şi organizatorice necesare pentru păstrarea confidenţialităţii şi integrităţii datelor cu caracter personal pe care le colectează.
Compania, reieşind din specificul activităţii, prin prezenta Politică, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecţie la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidenţă gestionate. În funcţie de acestea şi de categoriile de date cu caracter personal prelucrate (secţiunea 5.8. *infra*), Compania va clasifica informaţia care conţine date cu caracter personal astfel încât să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sunt prelucrate să fie localizate, indiferent de tipul purtătorului de date.
Compania va duce evidenţa documentaţiei cu privire la controalele de securitate efectuate în baza prezentei Politici.
În cadrul Companiei securitatea prelucrărilor de date cu caracter personal se va face numai cu respectarea şi observarea strictă a următoarelor dispoziţii:
A. Mijloace supuse principiilor de protecţie a datelor cu caracter personal
Protecţia datelor cu caracter personal în cadrul Companiei (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.
Sunt 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:
- suporturi magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;
- 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.
B. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin:
- preîntâmpinarea conexiunilor neautorizate la reţelele de telecomunicaţii şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele,
- împiedicarea accesului neautorizat la datele cu caracter personal prelucrate,
- preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program,
- preîntâmpinarea 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,
- preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, care este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea canalelor VPN,
- preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal, care este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor anti-virus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă,
- preîntâmpinarea scurgerii de informaţii ce conţin date cu caracter personal, care este asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent.
- stabilirea exactă a ordinii de acces la informaţia ce conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenţă instituite atât pentru utilizatorii interni cât şi pentru cei externi.
C. Măsurile generale de administrare a securităţii informaţionale

- În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.
- Computerele, terminalele de acces şi imprimantele sânt deconectate la terminarea sesiunilor de lucru.
- Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.
- 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.
- Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sânt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.
- Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.
- Este interzisă instalarea programelor de tip Shareware sau Freeware, fără aprobarea administratorului sistemului informatic.

5.1 Autorizarea accesului fizic

Accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale și/sau registrele ce conțin date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program, conform listei și însemnelor corespunzătoare (cartelele de identificare, cartelele cu microprocesoare, alte instrumente de acces aprobate de Companie), pentru preîntâmpinarea accesului persoanelor neautorizate.

Accesul neautorizat în perimetrul de securitate a încăperii (ilor) Companiei unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video este interzis, ținând cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 ale Legii privind protecția datelor cu caracter personal nr. 133 din 08.07.2011, precum și pct. 26 din Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

5.2. Administrarea și monitorizarea accesului fizic

Compania asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale și/sau la registrele de date cu caracter personal, inclusiv reacționează la încălcarea regimului de acces. Înainte de acordarea accesului fizic la sistemele informaționale și/sau la registrele de date cu caracter personal, se verifică drepturile de acces ale fiecărui solicitant.

Încăperile unde sunt instalate sistemele informaționale și/sau registrele de date cu caracter personal se echipează cu sisteme de control, securitate și asigurare a integrității corespunzătoare nivelului de protecție în dependență de tipul datelor prelucrate. Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

Sunt utilizate mijloace automatizate care asigură identificarea cazurilor de acces neautorizat și inițierea acțiunilor de blocare a accesului, precum și de stocare a informațiilor privind tentativele de acces neautorizat.

Accesul vizitatorilor (persoanelor terțe) se va asigura în conformitate cu regulile prevăzute de legislația în vigoare cu privire la protecția datelor cu caracter personal.

Perimetrul de securitate al Companiei este perimetrul oficiilor în care se prelucrează/stochează date cu caracter personal. Perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sunt rezistenți, intrările sunt echipate cu lacăte și semnalizare. Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc reprezentanții Companiei. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii Companiei sau în conformitate cu procedura stabilită în Regulamentul privind supravegherea prin mijloace video şi foto.

5.3 Asigurarea protecţiei datelor cu caracter personal

Salariaţii care în activitatea lor profesională intră în contact cu date considerate cu caracter personal sunt obligaţi să păstreze confidenţialitatea datelor şi să respecte întocmai prevederile Legii privind protecţia datelor cu caracter personal nr. 133 din 08.07.2011.

Obligaţia privind păstrarea confidenţialităţii datelor cu caracter personal rămâne valabilă şi în cazul trecerii într-un alt loc de muncă în cadrul Companiei sau după încetarea raportului de muncă.

Dispoziţiile prezentului articol se aplică, în acelaşi mod, pentru toate informaţiile deţinute de Companie referitoare la terţi, despre care salariatul ia cunoştinţa în cadrul activităţii sale.

5.4 Prelucrarea datelor cu caracter personal

Este interzisă prelucrarea datelor cu caracter personal fără consimţământul subiectului datelor cu caracter personal, cu excepţia cazurilor stabilite de legislaţia în vigoare.

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.

La încheierea operaţiunilor de prelucrare a datelor cu caracter personal, dacă subiectul acestor date nu şi-a dat consimţământul pentru o altă destinaţie, pentru stocare sau pentru o prelucrare ulterioară, acestea vor fi distruse, transferate sau transformate şi stocate conform legislaţiei în vigoare.

5.5 Identificarea şi autentificarea utilizatorului

Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal deţinută de Companie, trebuie să se identifice. Identificarea se va face prin introducerea unui cont de utilizator (sau „user-name") şi a parolei asociate respectivului cont de utilizator (parola de peste 8 caractere ce va fi formată din mai multe tipuri de caractere, respectiv cifre, litere şi caractere speciale).

Fiecărui utilizator ce i se va permite accesul la bazele de date cu caracter personal ale Companiei va avea propriul sau user-name şi parolă, care vor fi unice la nivelul Companiei. Administrarea identificatorilor utilizatorilor include (i) identificarea univocă a fiecărui utilizator, şi (ii) verificarea autenticităţii fiecărui utilizator.

User-name-urile nefolosite o perioadă mai îndelungată vor fi dezactivate şi distruse după un control prealabil intern al Companiei. Perioada după care conturile de utilizator vor fi dezactivate si distruse este de maxim 90 de zile de la data ultimului acces (login) a respectivului utilizator.

Compania asigură păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioada de un an) şi prevenirea folosirii repetate a acestora. 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 IT.

Orice cont de utilizator este însoţit de o modalitate de autentificare. Autentificarea va fi făcută prin introducerea unei parole asociate respectivului cont de utilizator (parola de peste 8 caractere ce va fi formată din mai multe tipuri de caractere, respectiv cifre, litere si caractere speciale), aceasta nefiind afişată în clar pe monitor. Parolele vor fi schimbate periodic, respectiv o dată la maxim 3 (trei) luni de la data primei folosiri a respectivei parole. Schimbarea periodică a parolelor urmează a fi efectuată numai de către utilizatori autorizaţi de persoana responsabilă a Companiei.

Toți utilizatorii se vor loga la bazele de date cu caracter personal ale Companiei având în vedere faptul ca sistemul informatic va refuza automat accesul utilizatorului după 3 (trei) introduceri greșite ale parolei.
Orice utilizator care primește un cont de utilizator și o parolă asociată este obligat să păstreze confidențialitatea strictă a acestora, în caz contrar urmând să răspundă disciplinar, pecuniar, penal, sau altfel conform legislației în vigoare.
Utilizatorii respectă regulile de asigurare a securității informaționale. În cazul alegerii și folosirii parolelor, aceste reguli includ:
- păstrarea confidențialității parolelor;
- interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;
- modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei;
- alegerea parolelor calitative cu o mărime de minimum 8 caractere, care nu sunt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sunt compuse integral din grupuri de cifre sau litere;
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).
Compania administrează și gestionează conturile de utilizator (și implicit parolele asociate) ținând cont de prezenta Politică.
Compania va autoriza doar anumiți utilizatori pentru a revoca sau a suspenda un cont de utilizator și parola asociată respectivului cont, dacă utilizatorul acestora și-a dat demisia ori a fost concediat, și-a încheiat contractul, a fost transferat la alt departament și noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată (mai mult de 3 luni).
Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste aprobate de persoana responsabilă a Companiei.
Drepturile de acces ale utilizatorilor la bazele de date cu caracter personal sunt revizuite/controlate cu regularitate (cel puțin la fiecare 6 luni) pentru asigurarea faptului ca nu au fost acordate drepturi de acces neautorizate și/sau după oricare schimbare de statut al utilizatorului. Controlul sistematic al acțiunilor utilizatorilor este, de asemenea, efectuat în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.
Accesul la funcțiile de securitate ale sistemelor informaționale de date cu caracter personal și la datele acestora este acordat în mod special doar persoanei responsabile a Companiei, desemnată conform prevederilor prezentei Politici.
5.6 Identificarea și autentificarea echipamentului
Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal, cu menținerea acestor informații pentru o perioadă rezonabilă.
5.7 Tipul de acces
Utilizatorii vor accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu. Pentru aceasta, un utilizator va primi un anumit tip de acces ce va fi stabilit, de la caz la caz, după:
I. funcționalitate (exemplu: administrare, introducere, prelucrare, salvare etc.); și
II. acțiuni aplicate asupra datelor cu caracter personal (exemplu: scriere, citire, ștergere).
Programatorii sistemelor (programelor pentru calculator) de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. În funcție de necesitate, Compania va permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.
Persoanele care asigură suportul tehnic vor putea avea acces la datele cu caracter personal pentru rezolvarea unor cazuri excepționale și numai cu aprobarea prealabilă expresă a persoanei

responsabile a Companiei, cu informarea subiectului datelor cu caracter personal respectiv (ale cărui date vor fi accesate) și cu perfectarea documentară corespunzătoare a fiecărui caz de acces. Pentru activitatea de pregătire a utilizatorilor sau pentru realizarea de prezentări se vor folosi date anonime. Angajații care predau cursurile de pregătire vor folosi date cu caracter personal pe parcursul propriei lor pregătiri.
Compania va implementa modalitatea strictă prin care se vor distruge datele cu caracter personal. Autorizarea pentru distrugerea datelor cu caracter personal este limitată la un singur utilizator.
5.7.1 Accesul de la distanță
Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), și sunt documentate, supuse monitorizării și controlului.
Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este autorizată de persoanele responsabile ale Companiei și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.
5.7.1.2 Limitarea folosirii tehnologiilor fără fir
Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului.
Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.
Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale Companiei.
5.8 Colectarea datelor cu caracter personal
Compania colectează datele cu caracter personal de la subiecții datelor cu caracter personal, cu informarea acestora despre categoriile de date și scopul prelucrării datelor cu caracter personal. În acest sens, fiecare subiect al datelor cu caracter personal își exprimă consimțământul conform legislației în vigoare.
În conformitate cu prevederile prezentei Politici, Compania colectează și prelucrează următoarele categorii de date de la subiecții datelor cu caracter personal:
1. numele și prenumele;
2. sexul;
3. data și locul nașterii;
4. cetățenia;
5. IDNP;
6. imaginea;
7. situația familială;
8. datele bancare;
9. semnătura;
10. codul personal de asigurări sociale (CPAS);
11. codul asigurării medicale (CPAM);
12. numărul de telefon/fax;
13. numărul de telefon mobil;
14. adresa (domiciliului/reședinței);
15. adresa e-mail;
16. profesia și/sau locul de muncă;
17. formarea profesională – diplome – studii;
18. obișnuințele/preferințele/comportamentul.
În conformitate cu prevederile legislației în vigoare, subiectul datelor cu caracter personal este informat asupra drepturilor pe care le are în legătură cu prelucrarea datelor sale personale, în special despre:
- dreptul de acces la datele cu caracter personal;
- dreptul de intervenție asupra datelor cu caracter personal;
- dreptul de opoziție al subiectului datelor cu caracter personal;
- dreptul de a nu fi supus unei decizii individuale;

- accesul la justiție;
- alte drepturi.

În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecția datelor cu caracter personal nr. 133 din 08.07.2011, persoanei necesită a-i fi furnizate următoarele informații, exceptând cazul în care el deține deja informațiile respective:

- 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);*
- privind scopul concret al prelucrării datelor cu caracter personal colectate;
- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existența drepturilor la informare și de acces la datele colectate; de intervenție asupra datelor *(în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora)* și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate;
- dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sânt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.

Subiecților de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum și împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în fișele personale *(alte materiale),* cu excepția cazurilor în care solicitanții își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.

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

În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse legale (*acte de identitate, de stare civilă, resurse informaționale principale de stat etc.*), modificarea urmând a fi efectuată în toate sistemele informaționale și de evidență gestionate.

Compania va desemna utilizatorii autorizați pentru operațiunile de colectare și introducere de date cu caracter personal într-un sistem informațional, urmând ca orice modificare a datelor cu caracter personal să fie efectuată numai de către respectivii utilizatori autorizați desemnați de Companie.

Sistemul informațional din cadrul Companiei înregistrează, în permanență, cine a făcut modificarea, data și ora modificării și asigură menținerea în mod separat a datelor șterse sau modificate, fără ca acestea din urmă să interfereze în vreun fel cu informațiile actualizate.

Datele personale ale subiecților datelor cu caracter personal sunt supuse următoarelor metode de prelucrare: colectare, înregistrare, organizare, stocare, păstrare, restabilire, adaptare ori modificare, extragere, consultare, utilizare, dezvăluire prin transmitere, diseminare sau în orice alt mod, alăturare ori combinare, blocare, ștergere sau distrugere, transmitere către autoritățile publice competente în conformitate cu legislația în vigoare și transmitere transfrontalieră.

Datele personale pot fi dezvăluite, în condițiile legii, către subiecții datelor cu caracter personal, autorități publice centrale/locale, servicii sociale sau de sănătate, reprezentanții legali ai subiecților datelor cu caracter personal, alte entități care oferă garanții suficiente de protecție a datelor personale.

Prelucrarea datelor cu caracter personal de către Companie va fi efectuată pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care acestea sunt prelucrate. După expirarea

acestei perioade, datele cu caracter personal vor fi păstrate în formă arhivată în conformitate cu Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova, aprobat prin Ordinul nr. 57 din 27.07.2016 al Serviciului de Stat de Arhivă.

5.8.1 Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate

Stocarea şi păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sunt conectate la internet, nu sunt echipate cu mijloace de protecţie speciale tehnice şi de program şi nu au instalate programe licenţiate, programe anti-virus, sisteme de control al securităţii soft-ului, de asigurare a efectuării periodice a copiilor de siguranţă şi de efectuare a auditului - este interzisă.

Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă. Accesul la computerele din dotare este protejat/restricţionat prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredinţate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul Companiei.

Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

5.9 Dezvăluirea datelor cu caracter personal

Dezvăluirea datelor cu caracter personal conţinute în format electronic în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informaţii 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 autorizaţi.

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 reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere *(expediere poştală cu aviz recomandat, înmânarea personală, etc.*).

Dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, *(spre exemplu: expedierea informaţiei prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.)* sunt interzise.

Sunt interzise operaţiunile de dezvăluire a datelor cu caracter personal între Companie şi alte entităţi care sunt amplasate geografic pe teritoriul Republicii Moldova din stânga Nistrului şi 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.

Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hârtie şi/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituţional/acord bilateral luându-se în considerare necesitatea asigurării unui nivel adecvat de protecţie a datelor cu caracter personal.

Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecţia datelor cu caracter personal nr. 133 din 08.07.2011, în special în cazurile când tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

Acces la sistemele informaționale gestionate în cadrul Companiei, din partea Procuraturii Generale *(după caz procuraturile teritoriale/specializate)*, Ministerului Afacerilor Interne, Centrului Național Anticorupție și alte asemenea autorități, va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi art. 212 din Codul de procedură penală.
În conformitate cu prevederile art. 157 din Codul de procedură penală, documentele în orice formă *(scrisă, audio, video, electronică etc.)* care provin de la persoane oficiale fizice sau juridice dacă în ele sunt expuse ori adeverite 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. Totodată, conform art. 214 din Codul de procedură penală, în cursul procesului penal nu pot fi administrate, utilizate şi răspândite 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.
În conformitate cu prevederile art.8 al Legii privind accesul la informație nr. 982 din 11.05.2000, datele cu caracter personal fac parte din categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

5.10 Execuția copiilor de siguranță

La nivelul Companiei se realizează copii de siguranță ale bazelor de date cu caracter personal și ale programelor folosite pentru prelucrările automatizate odată la 11 luni. Utilizatorii care execută aceste copii de siguranță sunt numiți în mod direct de persoana responsabilă a Companiei, numărul acestora fiind limitat la 1 (o) singură persoană. Copiile de siguranță sunt stocate în alte camere, în dulapuri/casete bancare.

5.11 Calculatoarele și alte terminale de acces

Calculatoarele și alte terminale de acces sunt instalate în încăperi cu acces limitat, care se pot încuia.
În cazul monitoarelor pe al căror ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă de maxim 15 (cincisprezece) minute, sesiunea de lucru se închide automat. Terminalele de acces folosite în relația cu publicul, pe care apar date cu caracter personal, sunt poziționate astfel încât nu pot fi văzute de public și după o perioadă de maxim 15 (cincisprezece) minute în care nu se acționează asupra lor, sesiunea de lucru se închide automat.

5.12 Fișierele de acces

Orice accesare a bazei de date cu caracter personal este înregistrată fie într-un fișier de acces (sau „log" în cazul prelucrărilor automate), fie într-un registru pentru prelucrările manuale de date cu caracter personal. Informațiile înregistrate în fișierul de acces sau în registru sunt următoarele:
a. contul de utilizator (numele și prenumele utilizatorului pentru bazele de date manuale);
b. numele fișierului accesat ori a fișei;
c. numărul înregistrărilor efectuate;
d. tipul de acces;
e. codul operației executate sau programul folosit;
f. data accesului (an, luna, zi):
g. timpul (ora, minutul, secunda).
În cazul prelucrărilor automate toate aceste informații vor fi stocate într-un fișier de acces general. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată conform următorilor parametri:
a. data și timpul tentativei intrării/ieșirii;

b. contul de utilizator (numele şi prenumele utilizatorului pentru bazele de date cu caracter personal manuale);
c. rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.
Este efectuată 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;
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:
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.
Compania va păstra fişierele de acces cel puţin 2 (doi) ani, pentru a fi folosite ca probe în cazul unor investigaţii. Daca investigaţiile se prelungesc, aceste fişiere se vor păstra atât timp cât se va considera necesar.
Fişierele de acces asigură identificarea de către persoana responsabilă a Companiei, a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancţiuni sau a sesizării organelor competente, după caz.
5.13 Sistemele de telecomunicaţii
Compania efectuează periodic (o dată la 6 luni) controlul autentificărilor şi tipurilor de acces pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea sistemelor de telecomunicaţii.
Sistemul de telecomunicaţii al Companiei este astfel conceput încât datele cu caracter personal nu pot fi interceptate sau transmise de oriunde. Ca şi măsură alternativă de siguranţă, utilizatorul este obligat să folosească metoda de criptare pentru transmisia datelor cu caracter personal existentă la nivelul Companiei la data transmiterii.
De asemenea, prin sistemele de telecomunicaţii se vor transmite numai datele cu caracter personal în cazurile strict necesare.
5.14 Instruirea personalului
În cadrul cursurilor de pregătire a utilizatorilor, Compania îi informează pe aceştia cu privire la:
i. prevederile Legii privind protecţia datelor cu caracter personal nr. 133 din 08.07.2011;
ii. cerinţele minime de securitate a prelucrărilor de date cu caracter personal stabilite de prezenta Politică; precum şi
iii. riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii utilizatorului.
Utilizatorii care au acces la date cu caracter personal sunt instruiţi de către Companie asupra confidenţialităţii acestora şi sunt avertizaţi prin mesaje care apar pe monitoare în timpul activităţii.
Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă.
Personalul care asigură exploatarea sistemelor informaţionale şi/sau a registrelor de date cu caracter personal trece, minimum o dată pe an, instruirea corespunzătoare referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate din domeniul protecţiei datelor cu caracter personal.
5.15 Folosirea calculatoarelor
Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva virusilor informatici) Compania impune următoarele măsuri:
a. utilizatorii nu folosesc programe software care provin din surse externe sau dubioase;
b. utilizatorii sunt informaţi în permanenţă cu privire la pericolul privind virusii informatici:

c. Compania are implementat un sistem centralizat, automat de devirusare şi de securitate a sistemelor sale informatice precum şi utilizează mijloace tehnice de constatare a atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaționale sau de preluare neautorizată a datelor cu caracter personal (Phishing);
d. la toate stațiile pe al căror monitor sunt afişate (în special) date cu caracter personal, este dezactivată în mod intenționat tasta „*Print Screen*" pentru a se evita astfel imprimarea respectivelor date, fie aceasta intenționată, fie din imprudență.

5.16 Securitatea electromagnetică

Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancționate, prin montarea lor în nişe speciale.
În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component IT.

5.17 Controlul instalării şi dezinstalării componentelor IT

Este exercitat controlul şi evidența instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.
Informațiile, care conțin date cu caracter personal şi care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitându-se folosirea funcțiilor standarde de nimicire.

5.18 Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal

Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

5.19 Imprimarea datelor

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune în mod expres de către persoana responsabilă a Companiei, în conformitate cu procedurile interne specifice ale Companiei privind folosirea şi distrugerea acestor materiale.

5.20 Marcarea documentelor

Informația ieşită din sistem, care conține date cu caracter personal, se marchează, indicându-se prescripții pentru prelucrarea ulterioară şi răspândirea acesteia, inclusiv indicându-se numărul de identificare unic al deținătorului de date cu caracter personal, după cum urmează: "*Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr. [•], înregistrat în Registrul de evidență al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr.133 din 08.07.2011 privind protecția datelor cu caracter personal.*"
În cazul în care consideră de cuviință şi în funcție de importanța datelor cu caracter personal prelucrate, Compania îşi rezervă dreptul de a impune şi alte măsuri de securitate suplimentare ce vor face parte integrantă din prezenta Politică, inclusiv prin aplicarea prevederilor ei în privința potențialilor subiecți ai datelor cu caracter personal care au comunicat Companiei datele lor cu caracter personal.

5.21 Incidente de securitate

Personalul Companiei informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.
În cazul producerii incidentelor de securitate în cadrul Companiei, persoana responsabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate cu informarea, în termen de 72

ore din momentul producerii incidentului de securitate, a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.
În cadrul controalelor, Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar și asigura accesul la informațiile necesare relevante obiectului controlului, conform prevederilor legale în vigoare.
Incidentele de securitate a sistemelor informaționale de date cu caracter personal se urmăresc și se documentează în regim permanent. Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.
Persoana responsabilă de implementarea prezentei Politici efectuează controale lunare pentru asigurarea respectării tuturor regulilor de securitate a datelor cu caracter personal. În urma controalelor dacă se constată careva abateri/incidente se întocmește un raport cu privire la cele stabilite.
Până la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova despre incidentele de securitate constatate.
Prezenta Politică este revizuită cel puțin o dată în an și aprobată la cel mai înalt nivel. Ea este adusă la cunoștința utilizatorilor și a salariaților Companiei care au tangență cu prelucrarea datelor cu caracter personal.
5.22 Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată
Compania, persoana împuternicită de către operator, persoanele terțe după caz, 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).

Secretarul Consiliului Caras Ghenadie