POLITICA DE SECURITATE
PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL A „NEW POST INTERNATIONAL MLD" SRL

Prezenta Politică privind prelucrarea datelor cu caracter personal (în continuare „**Politica**") a fost elaborată și aprobată de NEW POST INTERNATIONAL MLD SRL, IDNO 1014600029674 cu adresa juridică înregistrată pe bd. Ștefan cel Mare, 65, of. 806, mun. Chișinău, Republica Moldova (în continuare „**Operator**"), o companie care există și funcționează în conformitate cu legislația Republicii Moldova, în vederea corespunderii cu prevederile *Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal* și a cerințelor față de prelucrarea criptografică și asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010, precum și întru respectarea prevederilor altor reglementări aferente protecției datelor cu caracter personal a persoanei vizate, cu privire la următoarele:

1. SFERA DE APLICARE

1. Această Politică reprezintă un act de ordine interioară, care este obligatoriu pentru Operator, salariații și prepușii Operatorului. Operatorul va comunica prin plasarea la vedere conținutul acestei Politici tuturor salariaților săi. Conținutul acestei Politici va fi plasat la vederea Clienților Operatorului prin plasarea pe portalul web www.novaposhta.md.
2. Prezenta Politică se aplică și este obligatorie pentru toate activitățile operaționale ale Companiei care implică prelucrarea datelor cu caracter personal, dar fără a se limita la: - prelucrarea datelor despre Salariați, prelucrarea datelor despre Clienți/furnizori/subcontractanți; prelucrarea datelor prin mijloace de supraveghere video și prelucrarea datelor în cadrul evidenței contabile.

3. Salariații și prepușii Operatorului vor prelucra date cu caracter personal, cu respectarea principiilor și regulilor menționate în prezenta Politică, în scopuri legitime.

2. SCOPUL

1. Scopul elaborării prezentei Politici este de a defini cerințele și procedura de protecție a Datelor cu caracter personal împotriva scurgerilor neautorizate și de a respecta regulile de prelucrare a Datelor cu caracter personal, pentru a se asigura protecția vieții private a subiecților.

2. Sistemul de contabilitate și pontaj, datele despre salariați, clienți și furnizori, precum și oricare alte date prelucrate în corespundere cu prezenta Politică, sunt păstrate pe serverele Operatorului. Datele sunt **transferate transfrontalier** în Ucraina către Compania ООО Нова Пошта (New Post S.R.L.) în baza Contractului de transfer a datelor cu caracter personal încheiat.

3. Datele gestionate în cadrul acestui sistem sunt păstrate pe serverele Operatorului pentru a fi stocate pe serverele localizate la adresa înregistrată a Importatorului de date pentru îndeplinirea scopurilor de stocare și recuperare a datelor ca urmare a colectării informațiile generate ca urmarea încheierii contractelor cu clienții, precum și în scopuri statistice. Datele sunt stocate pe servere atât timp cât este necesar în temeiul contractului încheiat. În cazul în care contractul transfrontalier este încetat, suspendat sau sub o altă formă nu este posibil stocarea datelor în afara jurisdicției Republicii Moldova de către Exportatorul de date, atunci Operatorul va suspenda temporar transferul datelor. În oricare caz de încetare, părțile acordului de transfer transfrontalier își vor păstra drepturile și obligațiilor în privința datelor personale transferate. Datele sunt **transferate transfrontalier** în Ucraina.
4. Datele cu caracter personal înregistrate în prezentul sistem de evidență vor fi stocate pe serverele Operatorului, care sunt amplasate în afara Republicii Moldova. În acest sens, Operatorul a încheiat un Acord de transfer transfrontalier a datelor cu caracter personal cu Operatorul străin împuternicit, care să reglementeze detaliat condițiile și detaliile la transferul datelor cu caracter personal, fiind reglementate drepturile și obligațiile importatorului și exportatorului de date. În special, Importatorul

de date are obligația de a procesa datele cu caracter personal numai în condițiile și conform instrucțiunilor exportatorului de date.

5. **Următoarele categorii de date vor fi supuse transferului:** Datele cu caracter personal se referă la următoarele categorii de date: numele, prenumele și patronimicul; Sexul ,Semnătura, Semnătura electronică, numărul personal de identificare de stat (IDNP); data și locul nașterii; cetățenia, datele din actele de stare civilă, codul personal de asigurări medicale (CPAM), telefon mobil, adresă domiciliu/reședință telefon/ fax, email profesie, funcție formare profesională - diplome - studii situație familială datele membrilor de familie situație economică sau financiară, mărimea salariului brut, premii, sporuri, suplimente, stimulări, date din certificatul de concediu medical, date bancare imagine date din permisul de conducere sancțiuni disciplinare codul personal de asigurări sociale (CPAS) codul personal al asigurării medicale date din certificate de înmatriculare locul de muncă.
6. Subiectul datelor cu caracter personal, va fi informat cu privire la transferul datelor, și cu privire la drepturile acestuia. Transmiterea transfrontalieră a datelor are loc cu acordul expres a Subiectului de date. Consimțământul privind transmiterea transfrontalieră va fi incorporat în Contractul Individual de Muncă, sub forma unui consimțământ exprimat expres. Modelul consimțământului privind transmiterea transfrontalieră a datelor este anexat la prezenta Politica. Factura poștală prin care se prelucrează datele Clienților este anexată la prezenta Politica.
7. Atât exportatorul de date, cât și importatorul de date va asigura respectarea strictă a drepturilor subiectului de date. În această odine de idei, subiecților de date le vor fi, în mod direct sau prin intermediul unei părți terțe, furnizate informațiile personale despre ei în cazul în care o organizație deține, cu excepția cererilor care sunt vădit abuzive. Sursele de date cu caracter personal nu trebuie să fie identificate atunci când acest lucru nu este posibil, prin eforturi rezonabile, sau în cazul în care drepturile altor persoane decât individul s-ar fi încălcat. Subiecții de date trebuie să fie capabili de a avea informațiile cu caracter personal despre ei rectificate, cu modificările ulterioare, sau șterse în cazul în care sunt inexacte sau prelucrate împotriva acestor principii. În cazul în care există motive întemeiate de a pune la îndoială legitimitatea cererii, organizația poate cere justificări suplimentare înainte de a proceda la rectificare, modificare sau ștergere. Notificarea oricărei rectificări, modificări sau ștergeri a terților cărora le-au fost dezvăluite datele nu trebuie să fie făcută atunci când

acest lucru implică un efort disproporționat. O persoană trebuie să aibă, de asemenea, posibilitatea de a se opune la prelucrarea datelor cu caracter personal care o privesc, dacă există motive întemeiate și legitime legate de situația sa personală. Sarcina probei pentru orice refuz se pune pe seama importatorului de date, iar subiectul de date poate contesta întotdeauna un refuz în fața autorității

3. CATEGORII DE SUBIECȚI ȘI CATEGORII DE DATE

1. Operatorul în legătură cu activitatea sa prelucrează date cu caracter personal ale salariaților săi (curenți, candidați la angajare), precum și date care se referă la persoane fizice: parteneri, sub-contractanți și alți furnizori de bunuri și servicii ai Operatorului în limitele stabilite de legislație („**Subiecți**").

2. Categoriile de date personale prelucrate de Operator sunt prezentate în Anexa 1 la această Politică.

3. Operatorul prelucrează datele cu caracter personal cu utilizarea mijloacelor manuale și/sau automate, cu respectarea cerințelor legale și în condiții care să asigure securitatea, confidențialitatea și respectarea drepturilor subiecților.

4. PRINCIPII GENERALE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

1. Datele cu caracter personal sunt prelucrate:

a) corect și conform prevederilor legale - prelucrarea de date cu caracter personal se va efectua în strictă conformitate cu legislația din domeniul protecției datelor cu caracter personal. Acest fapt presupune că înainte de a colecta, utiliza și dezvălui datele cu caracter personal, prelucrarea trebuie să rezulte expres dintr-un drept sau obligație legală;

b) *în scopuri determinate, explicite și legitime, iar ulterior nu sunt prelucrate în scopuri incompatibile* - orice prelucrare de date cu caracter personal se face în scopuri bine determinate, explicite și legitime, adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate. Informațiile acumulate sunt destinate utilizării de către Operator și partenerii acestuia în scopuri legitime și pot fi comunicate, în funcție de necesitate, următorilor destinatari: părților co-contractante, notarilor publici, instanțelor de judecată, consultanți juridici și financiari, inclusiv avocați, furnizorilor de bunuri și servicii, instituțiilor publice, instituțiilor bancare, registrelor publice, precum și altor tipuri de destinatari direct vizați.

c) *confidențialitatea* - salariații Operatorului, care sunt antrenați în prelucrarea nemijlocită a datelor cu caracter personal sunt obligați să respecte confidențialitatea datelor personale prelucrate de Operator, în baza legii și/sau a contractelor corespunzătoare.

d) *consimțământul* - orice prelucrare de date cu caracter personal a Subiecților poate fi efectuată numai dacă aceștia și-au exprimat consimțământul pentru prelucrare, cu excepțiile prevăzute de lege.

e) *protejarea Subiecților* - subiecții au dreptul de acces la datele despre ei care sunt prelucrate de Operator, de intervenție asupra acestora, de opoziție și de a nu fi supus unei decizii individuale, precum și dreptul de a se adresa Centrului Național pentru Protecția Datelor cu Caracter Personal sau instanței de judecată pentru apărarea oricăror drepturi garantate de lege, care le-au fost încălcate. Limitarea acestor drepturi poate fi admisă în cazurile prevăzute de lege.

f) *securitatea* - Măsurile de securitate a datelor cu caracter personal sunt stabilite astfel încât să asigure un nivel adecvat de securitate a datelor cu caracter personal procesate de către Operator.

g) *adecvat, pertinent și neexcesiv* - orice prelucrare de date cu caracter personal trebuie să corespundă scopului pentru care au fost colectate și să fie pertinente și neexcesive în contextul scopului urmărit. În vederea

respectării acestor cerințe, operatorul aplică principiul minimizării datelor cu caracter personal, care constă în colectarea doar acelor informații care sunt strict necesare pentru realizarea serviciilor prestate. Evaluarea respectării acestor trebuințe se va efectua periodic și la necesitate.

h) *exacte și actualizate* - categoriile de date prelucrate de către operator sunt stabilite exhaustiv, fiind prelucrate doar date veridice. Operatorul verifică periodic datele cu caracter personal prelucrate, prin contrapunerea datelor prelucrate cu cele deținute de către subiecții de date.

i) *pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sânt colectate și ulterior prelucrate* - datele cu caracter personal se stochează doar pe perioada existenței raporturilor civile și/sau pe termenul expres stabilit de legislația specială în temeiul căreia sunt prelucrate datele cu caracter personal.

5. DREPTURILE SUBIECȚILOR DE DATE CU CARACTER PERSONAL

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

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

obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.

2. 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.

3. 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.

4. 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.

6. APLICAREA, COMPETENȚA ȘI DESTINATARII POLITICII

1. Prezenta Politică se aplică și este obligatorie pentru toate activitățile operaționale ale Companiei și se aduce la cunoștință salariaților și partenerilor Operatorului și este obligatorie pentru aceștia**.**

Persoana responsabilă

2. Operatorul, printr-un ordin semnat de persoana cu funcție de conducere, va desemna, din rândul salariaților săi, o persoană responsabilă pentru elaborarea, implementarea și monitorizarea respectării obligațiilor în domeniul protecției datelor cu caracter personal. Persoana responsabilă pentru protecția datelor cu caracter personal este jurisconsultul Companiei („**Persoana responsabilă**").

3. Atribuțiile persoanei responsabile:

a) realizează analiza de risc aferentă resurselor informaționale;
b) prevede măsurile de protecție logică;
c) asigură verificarea existenței, actualizării și suficienței licențelor pentru resursele informaționale;
d) asigură evidența auditului sistemelor informatice, precum și stocarea și accesibilitatea acestora pentru inspecție în conformitate cu regulamentele interne;
e) definește procedura prin care utilizatorii sistemului de informații beneficiază de dreptul de a accesa resursele informaționale și de a le gestiona și organizează controlul utilizării acestor resurse;
f) asigură producerea copiilor de rezervă a resurselor informaționale și stocarea acestora, precum și de renovarea resurselor informaționale în cazul în care funcționarea resurselor informaționale a fost perturbată sau imposibilă din cauza deteriorării resurselor tehnice sau din alte motive;
g) prevede măsuri de protecție fizică;
h) participă la analiza riscurilor, identifică amenințările sistemului informațional referitor la resursele tehnice și evaluează probabilitatea acestor amenințări;
i) asigură restaurarea resurselor tehnice în cazul în care au fost deteriorate.

4. Persoana responsabilă furnizează introducerea unor proceduri relevante de prelucrare a datelor, precum și realizarea de înregistrări de audieri pentru a înregistra\ actele de gestionare a Datelor cu caracter personal.
5. Persoana responsabilă cu protecția Datelor cu caracter personal asigură instruirea angajaților, precum și testarea cunoștințelor în domeniul protecției datelor cu caracter personal.

6. Persoana responsabilă va fi implicată în mod adecvat și în timp util în toate aspectele referitoare la protecția datelor cu caracter personal.
7. Operatorul sprijină persoana responsabilă în îndeplinirea sarcinilor sale, asigură resursele necesare pentru a permite specialistului în protecția datelor cu caracter personal să îndeplinească sarcinile descrise mai sus și oferă acces la Datele cu caracter personal și la actele de prelucrare a Datelor cu caracter personal, dar și posibilitatea de a actualiza cunoștințe speciale specialistului în domeniul protecției datelor.

8. Sarcinile persoanei responsabile în protecția datelor cu caracter personal:

a) să informeze și să consulte angajații care realizează prelucrarea Datelor cu caracter personal în ceea ce privește atribuțiile acestora în conformitate cu actele interne ale Operatorului și ale actelor normative privind protecția Datelor cu caracter personal;
b) să supravegheze respectarea actelor interne și externe de reglementare a protecției Datelor cu caracter personal, inclusiv divizarea sarcinilor, să informeze și să instruiască angajații implicați în acte de prelucrare a Datelor cu caracter personal;
c) la cerere, să ofere consultanță cu privire la Evaluarea Impactului asupra protecției Datelor cu caracter personal, să participe la pregătirea acestei evaluări și să supravegheze punerea sa în aplicare;
d) să elaboreze și să mențină registrul de încălcări a protecției Datelor cu caracter personal;
e) să coopereze cu Autoritatea de Supraveghere competentă și să fie contactul Autorității de Supraveghere cu privire la aspectele legate de prelucrarea Datelor cu caracter personal, inclusiv în legătură cu discuțiile prealabile și alte probleme;
f) să consulte Persoanele Vizate care au abordat specialistul în protecția datelor cu caracter personal în ceea ce privește prelucrarea Datelor cu caracter personal în cadrul Companiei.

9. Drepturile persoanei responsabile în protecția datelor cu caracter personal:

a) să colecteze informații pentru a identifica procesele de prelucrare a Datelor cu caracter personal, să analizeze și să verifice conformitatea

prelucrării Datelor cu caracter personal cu actele interne și să informeze, să ofere consultanță și recomandări în legătură cu prelucrarea Datelor cu caracter personal;

b) să realizeze auditul prelucrării Datelor cu caracter personal fără a asigura în prealabil o notificare;

c) să se familiarizeze cu documentele companiei, cerințele tehnice și organizatorice care afectează prelucrarea Datelor cu caracter personal, precum și să primească informații în timp util despre incidentele de securitate și să se familiarizeze cu Registrul incidentelor de securitate;

d) să participe la adoptarea de rezoluții care au ca obiect protecția Datelor cu caracter personal, să se familiarizeze cu documentele relevante pentru a-și exprima opinia și pentru a oferi sfaturi în acest sens.

7. COMPONENTELE SECURITĂȚII INFORMAȚIILOR

a) Operatorul este conștient de importanța și însemnătatea securității informaționale și definește componentele securității informațiilor și cerințele pe care angajații Operatorului trebuie să le îndeplinească în cadrul activităților zilnice de muncă.

b) Securitatea informațiilor se descrie prin confidențialitatea, integritatea și accesibilitatea acestora. Compania are grijă să se asigure că:

- informațiile să fie disponibile doar persoanelor autorizate să le primească (confidențialitate);
- informațiile și metodele lor de prelucrare sunt corecte și complete (integritate);
- utilizatorii autorizați au acces la informații în caz de nevoie (accesibilitate).

c) Compania implementează protecția tehnică a Datelor cu caracter personal prin mijloace fizice și logice de protecție, prin asigurarea protecției împotriva amenințării Datelor cu caracter personal cauzate de impactul fizic și prin protecția implementată prin mijloace de tehnologia informației (mijloace IT). Prin selectarea tipului de stocare a Datelor cu caracter personal se va lua în considerare posibilitatea ca daunele să fie cauzate de

incendii, inundații, explozii, precum și ca alte incidente de Securitate să fie cauzate de natură, IT și oameni.

d) Resursele tehnice care conțin Date cu caracter personal, inclusiv computerele desktop și cele portabile, hard disk-uri, atunci când nu sunt utilizate, sunt stocate în locuri care nu sunt ușor accesibile altor persoane (cum ar fi, în camere sau dulapuri încuiate).

8. CLASIFICAREA PROTECȚIEI DATELOR CU CARACTER PERSONAL ÎN CONFORMITATE CU NIVELUL ACESTORA, VALOAREA ȘI CONFIDENȚIALITATEA, REGISTRUL DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

8.1. În cadrul activității sale, Operatorul ține evidența mai multor date personale cum ar fi evidența salariaților, formatorilor, participanților la trening, partenerilor Operatorului, evidența contabilă, evidența vizitatorilor, altele, consemnându-le în registrele respective. Toate aceste registre conțin date cu caracter personal. Toate registrele, care conțin date cu caracter personal, se păstrează în locuri protejate în strictă conformitate cu prezentele reguli și se utilizează exclusiv în scopurile pentru care ele sunt create.

8.2. Registre de evidență

a) Operatorul întocmește și menține Registrul care este revizuit și completat regulat în conformitate cu prelucrarea efectivă a Datelor cu caracter personal, inclusiv revizuiri periodice ale termenelor de stocare a Datelor cu caracter personal definite în Registru.

b) Registrul este menținut în scopul înregistrării generale a actelor realizate cu Date cu caracter personal în cadrul unuia sau a mai multor scopuri, inclusiv înregistrarea și controlul destinatarilor Datelor cu caracter personal.

c) În caz de necesitate, Operatorul oferă acces la Registru Autorității de Supraveghere competente.

9.REGULI ȘI PROCEDEE DE SECURITATE

1. Accesul în sediu:

1.1. Conducerea Operatorului este conștientă de importanța și însemnătatea securității informaționale și definește cerințele pe care angajații Companiei trebuie să le îndeplinească în cadrul activităților zilnice de muncă.

1.2. Accesul în sediile/ birourile de lucru ale Operatorului, ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal prelucrate de Operator este restricționat, se efectuează în baza ecusoanelor sau cartelelor de identificare sau cheilor de acces, fiind permis doar salariaților Operatului, partenerilor și vizitatorilor autorizați ("**Utilizatori**"). Accesul vizitatorilor se înregistrează în registre, care se păstrează minimum un an. La expirarea termenului de păstrare, registrele se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă. Înainte de acordarea accesului fizic la sistemele informaționale de date cu caracter personal se verifică competențele de acces.

1.3. Se efectuează administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces. Registrele de monitorizare se păstrează minimum un an, la expirarea căruia acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă.

1.4. Computerele, serverele, alte terminale de acces se amplasează în locuri cu acces limitat pentru persoane străine.

2. Administrarea conturilor de acces (account-urilor)

2.1. Administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora este administrată de către Operator. La administrare sânt folosite mijloace automatizate de suport. Acțiunea

conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp (pentru fiecare tip de cont de acces în parte). Sânt dezactivate automat, după o perioadă de maximum trei luni, conturile de acces ale utilizatorilor neactivi, care prelucrează date cu caracter personal. Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

2.2. În spațiile de ședință destinate publicului, se va minimiza în măsura posibilității activitățile de prelucrare a datelor cu caracter personal, iar mijloacele și echipamentele care oferă acces la datele prelucrate de Operator vor fi securizate.

2.3. Computerele, serverele, alte terminale de acces se amplasează în locuri cu acces limitat pentru persoane străine.

3. Integritatea perimetrului

3.1. Perimetrul biroului Operatorului este determinat concret și clar. Perimetrul clădirii sau încăperii în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal trebuie să fie integru din punct de vedere fizic. Pereții exteriori ai încăperilor trebuie să fie rezistenți, intrările echipate cu lacăte.

4. Măsuri pentru a proteja resursele tehnice împotriva situațiilor de urgență (incendii, inundații):

4.1. Pentru a asigura protecția centrului de date a fost construit un sistem modern de stingere a incendiilor. Starea securității la incendiu la centrul de date este supravegheată de Administrator.

4.2. Un computer unde sunt stocate informații cu un anumit grad de confidențialitate poate să nu fie conectat la rețelele externe ale rețelei locale din care pot fi accesate rețelele externe.

4.3. Informațiile despre un nivel special de confidențialitate nu sunt transmise prin intermediul rețelelor externe.

4.4. În cazul în care computerele care dețin informații cu un anumit nivel de confidențialitate sunt conectate la rețeaua locală, cablurile rețelei locale nu pot traversa teritoriul unde protecția fizică relevantă împotriva unei amenințări la adresa sistemului informatic nu este furnizată, iar dispozitivele de rețea ar trebui să fie localizat în incinte cu protecție fizică corespunzătoare pentru o amenințare la adresa sistemului informatic.

4.5. Protecția datelor clienților împotriva accesului neautorizat se asigură de: 24/7 sisteme de alarmă și sisteme de supraveghere la nivel înalt.

5. Auditul securității

5.1. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

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

5.2. Este efectuată și înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:

a) data și timpul tentativei de pornire;
b) denumirea/identificatorul programului aplicativ sau procesului;
c) ID-ul utilizatorului;
d) rezultatul tentativei de pornire - pozitivă sau negativă.

5.3. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

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

5.4. Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
a) data și timpul modificării competențelor;
b) ID-ul administratorului care a efectuat modificările;
c) ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

5.5. Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
a) data și timpul eliberării;
b) denumirea informației și căile de acces la aceasta;
c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
d) ID-ul utilizatorului, care a solicitat informația;
e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) și rezultatul eliberării - pozitiv sau negativ.

6. Păstrarea datelor de audit

6.1. Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal, în scopul depistării activităților neobișnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la

cazurile depistării acestor activități. Durata stocării rezultatelor auditului securității în sistemele informaționale de date cu caracter personal este de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare.

7. ANTIVIRUS

7.1. Operatorul și salariații vor asigura protecția contra infiltrării programelor dăunătoare (virușilor) în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare. Totodată, Operatorul și salariații vor utiliza tehnologii și mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaționale de date cu caracter personal și constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaționale. Se asigură identificarea, înregistrarea și înlăturarea deficiențelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestor soft-uri. Se exercită controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal. Soft-urile destinate prelucrării datelor cu caracter personal și informația care conține date cu caracter personal, accesul la care se efectuează prin intermediul sistemelor de acces public, sânt securizate prin metoda folosirii semnăturii digitale/mobile.

8. COPII DE REZERVĂ

8.1. O dată în an Operatorul va asigura executarea copiilor de siguranță a informațiilor care conțin date cu caracter personal și copiile soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal. Copiile de rezervă se păstrează în locuri protejate, în afara zonei de amplasare a acestei informații. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației care conține date cu caracter personal. Procedurile de restabilire a copiilor de

siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

9. VERIFICĂRI INTERNE

9.1. Cel puțin o dată în an se verifică îndeplinirea măsurilor tehnice și/sau organizaționale luate pentru detectarea unor disfuncționalități în ceea ce privește folosirea în procesul prelucrării datelor cu caracter personal a sistemelor de telecomunicații și/sau efectuarea îmbunătățirilor, în caz de necesitate. Controalele de securitate sânt actualizate de fiecare dată. În funcție de rezultatele Controalelor de securitate, Operatorul datelor cu caracter personal întreprinde măsuri de reorganizare a proceselor sau își schimbă infrastructura.

10. Integritatea echipamentului

10.1. Operatorul și salariații acestuia vor asigura securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, a router-elor, întrerupătoarelor, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. Cablurile de rețea, prin care se efectuează operațiuni de prelucrare a datelor cu caracter personal, trebuie protejate contra conectărilor nesancționate sau deteriorărilor.

10.2. Deconectare la nevoie are loc în cazul apariției situațiilor excepționale, de avarie sau de forță majoră, trebuie asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component de tehnologie informațională.

10.3. Salariații Operatorului vor deconecta computerele, terminalele de acces și imprimantele la terminarea sesiunilor de lucru.

10.4. Folosirea UPS: Operatorul va prevedea surse autonome de alimentare cu energie electrică de scurtă durată, folosite pentru terminarea corectă a

sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

1. Parole

Operatorul și salariații acestuia vor respecta următoarele reguli de asigurare a securității informaționale în cazul alegerii și folosirii parolelor:

a) păstrarea confidențialității parolelor;
b) este interzisă înscrierea parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia, parolele se păstrează în formă cifrată, utilizîndu-se algoritmul criptografic unilateral (funcția hash);
c) modificarea parolelor o dată la maxim 3 luni și de fiecare dată când sunt prezenți indicii unei eventuale compromiteri a sistemului sau parolei;
d) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sânt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sînt compuse integral din grupuri de cifre sau litere;
e) dezactivarea procesului automatizat de înregistrare a parolei (cu folosirea parolelor salvate);
f) este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora;
g) accesul este blocat după trei tentative greșite de autentificare;
h) la momentul introducerii, parolele nu se reflectă clar pe monitor;
i) după instalarea sistemului, se schimbă informațiile de autentificare a utilizatorilor utilizate standard;
j) este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioadă de un an) și prevenirea folosirii repetate a acestora.

10.1. În cazul în care contractul care reglementează relațiile dintre Operator și utilizator a fost încetat, suspendat sau modificat și 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 și autentificare se revocă sau se

suspendă. Contul de utilizator inactiv (inacțiune în perioada de maximum 2 luni) se dezactivează;

10.2. Accesul la funcțiile de securitate ale sistemelor informaționale de date cu caracter personal și la datele acestora este acordat doar persoanei responsabile.

10.3. Utilizatorii sistemelor informaționale de date cu caracter personal se învestesc doar cu acele drepturi/competențe, care sînt necesare pentru realizarea de către ei a obiectivelor stabilite acestora. Drepturile de acces ale utilizatorilor la sistemele informaționale de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare șase luni) și după oricare schimbare de statut al utilizatorului. Accesul la informații și resurse este acordat în baza principiului „necesitatea de a avea acces la informație". Sistemele sunt proiectate cu un minim necesar de informație pentru activitate. Utilizatorii sunt asigurați cu cel mai inferior nivel de acces, necesar pentru îndeplinirea atribuțiilor de funcție.

10.4. Securizarea accesului de la distanță:Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal ale Operatorului sânt securizate cu utilizarea VPN, criptării, cifrării, precum și a altor metode de securizare, precum și vor fi documentate, supuse monitorizării și controlului de către Operator. Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal se autorizează de conducătorul Operatorului și/sau de persoana responsabilă a Operatorului desemnată de conducător conform prezentei Politici și se permite doar Utilizatorilor, cărora accesul respectiv le este necesar pentru îndeplinirea obiectivelor profesionale stabilite.

10.5. Accesul la dispozitive electronice (telefoane mobile, tablete, laptopuri etc.): Folosirea echipamentului portativ și mobil care permit accesul la sistemele informaționale de date cu caracter personal ale Operatorului trebuie autorizată de conducătorul Operatorului sau de persoana responsabilă desemnată de conducător.

11. ACCES LA INTERNET ȘI EMAIL

1. Sistemele de poștă electronică și Internetul sunt mijloace rapide și eficiente de comunicare și colectare de informații. Ambele tipuri de conexiuni aparțin Operatorului și sunt puse la dispoziția salariaților acestuia ca mijloace de comunicare și informare eficiente, pentru a fi folosite în cursul și în scopul realizării activității profesionale. Rețelele de internet fără fir (wifi) gestionate de Operator este protejată cu parolă. Accesul la această parola poate fi oferit de conducătorul Operatorului.

2. În scopul de a asigura securitatea rețelei informatice, dar și pentru a preveni utilizarea necorespunzătoare a accesului la Internet, o serie de date de trafic sunt reținute în mod automat (fără intervenție umană), continuu și pentru orice calculator aflat în rețeaua locală a Operatorului. De regulă, aceste informații sunt stocate pentru o perioadă de câteva săptămâni sau luni, după care sunt șterse definitiv prin suprascriere. Reținerea datelor de trafic nu se face în scopul monitorizării salariaților Operatorului. Cu toate acestea, Operatorul poate analiza înregistrările existente la un moment dat cu privire la un anumit salariat, vizitator comunicând acestuia atât efectuarea analizei în cauză, cât și motivele acesteia.

3. Atenție la atașamente. Emailurile sunt mijlocul principal prin care se pot introduce viruși în rețeaua locală, motiv pentru care întreg colectivul de muncă precum și orice persoană care va obține acces la resursele informaționale ale Operatorului trebuie să manifeste grijă la deschiderea atașamentelor, în special în cazul în care proveniența acestora este neclară / nesigură / suspectă sau extensia fișierului este .exe.

4. Despre mesaje private. Mesajele electronice și documentele atașate la acestea folosite de salariații. Operatorilor folosind mesageria de serviciu nu sunt private atât timp cât sunt create și/sau stocate pe calculatorul de serviciu. O copie de siguranță a tuturor emailurilor transmise sau primite de pe sau pe adresele profesionale, de regulă, este păstrată pe serverul Operatorului.

5. Despre emailuri gratuite. Internetul oferă multe opțiuni de comunicare electronică gratuită, cum sunt @gmail.com, @yahoo.com, @mail.ru, etc. Operatorul avertizează că aceste sisteme de comunicare electronică nu corespund cerințelor de protecție a datelor cu caracter personal. Salariații Operatorului se vor abține de la transmiterea datelor personale ale Subiecților prin asemenea sisteme de comunicare. Operatorul garantează că are creat un sistem de comunicare electronică corporativă, care este protejată în strictă conformitate cu prezentele reguli și Legea privind protecția datelor cu caracter personal.

12. PROCEDURA DE STOCARE ȘI DISTRUGERE A DATELOR CU CARACTER PERSONAL, A SUPORTURILOR DE INFORMAȚII

12.1. Suporturile de informații de la centrul de date în care sunt stocate datele Subiecților și care sunt deteriorate sau uzate trebuie păstrate într-un loc sigur în centrul de date după deconectarea lor de la software-ul centrului de date.

12.2. Datele Subiecților sunt distruse atunci când termenul de stocare a acestora este definit în conformitate cu legislația aplicabilă, Regulamentul Intern al Operatorului și este stabilit în termenul de expirare al Registrului.

12.3. Stocarea datelor cu caracter personal are loc pe fișiere electronice și pe hârtie. Fișierele electronice și cele de hârtie care conțin Date cu caracter personal sunt stocate pentru termenul definit prin Registru.

12.4. Accesul în spațiile/perimetrul unde sunt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale /regulamentelor departamentale aprobate.

12.5. Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sunt conectate la internet, nu sunt echipate cu mijloace de protecție speciale

tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă.

12.6. Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul Companiei.

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

12.8. Compania revizuiește condițiile de stocare ale Datelor cu caracter personal definite de Registru după cum este necesar, cu toate acestea, minim o dată la 2 (doi) ani.

12.9. În cursul evaluării termenilor de stocare a Datelor cu caracter personal, Compania va lua în considerare cel puțin următoarele aspecte:

a) Datele cu caracter personal sunt stocate cel puțin până când sunt necesare pentru a atinge scopul prelucrării;

b) Condițiile de stocare a Datelor cu caracter personal sunt aliniate la termenii de stocare definiți de legislație în conformitate cu scopul de stocare a Datelor cu caracter personal;

c) Datele cu caracter personal sunt stocate atât timp cât Compania trebuie să păstreze dovezile în cazul inițierii unei reclamații legale și/sau a unui litigiu;

d) Datele cu caracter personal nu pot fi șterse din documente dacă acestea afectează forța juridică a documentului.

13. TERMEN DE PĂSTRARE A DATELOR

13.1. Datele personale prelucrate în cadrul exercitării activității Operatorului se vor păstra pe toată perioada contractuală (angajării salariatului, prestării serviciului/ achiziției materialelor etc., de către/către Operator), precum și pe durata necesară realizării scopurilor pentru care au fost colectate sau protejării intereselor legitime ale Operatorului, unităților afiliate acestuia și/sau salariaților și asociaților acesteia.

13.2. După expirarea termenului legal/contractual de păstrare, Datele cu caracter personal și/sau documentele pe suport electronic sau de hârtie sunt distruse, anonime sau transferate arhivelor de stat în situații specifice. Fiecare Persoană Responsabilă de procesul de prelucrare a Datelor cu caracter personal este responsabilă cu implementarea ștergerii sau cu procesul de anonimizare.

13.3. La încetarea raporturilor care stau la baza prelucrării datelor Subiecților de către Operator, purtătorii de date cu caracter personal se transmit în arhiva Operatorului și se păstrează pe durata următoarelor termene de păstrare:

- datele personale despre sau obținute de la parteneri și contractanți: 5 ani de la expirarea raporturilor stabilite;

- datele personale cu privire la salariați: 75 ani de la încetarea contractelor individuale de muncă.

13.4. Termenul de păstrare poate fi diferit de cel indicat, dacă un termen diferit de păstrare este indicat în indicatorul documentelor-tip și a termenelor lor de păstrare pentru organizațiile și întreprinderile RM. În asemenea caz datele se vor păstra pe perioada indicată în indicatorul documentelor-tip. În caz de litigiu datele se vor prelucra pe toată durata

necesară apărării intereselor legitime ale Operatorului și persoanelor asociate acestuia.

14. ȘTERGEREA ȘI DISTRUGEREA DATELOR CU CARACTER PERSONAL

14.1. Informațiile care conțin date personale și nu mai sunt necesare pentru atingerea scopurilor de prelucrare definite de Companie și a căror stocare nu este prevăzută de legislația aplicabilă ar trebui distruse. Informațiile electronice sunt distruse astfel încât să nu fie posibilă restaurarea fișierelor informative. Informațiile scrise (pe suport de hârtie) sunt distruse în așa fel încât informațiile conținute în acestea să nu fie restaurate.

14.2. Este interzisă transferarea (înstrăinarea) dispozitivelor informatice către părți terțe dacă conțin Date cu caracter personal. Interdicția de mai sus ar trebui, de asemenea, să fie respectată în cazurile în care dispozitivele IT sunt transferate pentru utilizare. Dacă un dispozitiv IT are nevoie de o reparație în cadrul garanției, înainte de a fi livrat pentru reparații, securitatea Datelor personale conținute de acesta trebuie asigurată.

14.3. Datele cu caracter personal care au devenit incomplete, învechite, falsificate, procesate ilegal sau care nu mai sunt necesare pentru atingerea scopului prelucrării Datelor cu caracter personal definite de Companie sunt imediat rectificate, actualizate sau șterse.

14.4. La încheierea procesului de prelucrare a Datelor cu caracter personal și/sau la expirarea termenului de stocare a acestora, în cazul în care Datele cu caracter personal nu sunt anonime, Compania sau Persoana Autorizată va șterge Datele personale din Sistemul de Informații astfel încât acestea să nu mai poată fi recuperate.

14.5. Documentele în format de hârtie care conțin Date cu caracter personal sau ciornele acestora sunt distruse în conformitate cu procedura definită de legislație după prelucrarea datelor și/sau expirarea termenului de stocare, dacă acestea nu sunt transferate în arhivă.

14.6. După terminarea necesității utilizării lor, resursele tehnice care conțin date personale (USB, CD, HDD etc.) sunt transferate Departamentului de Tehnologii Informaționale al Companiei, care distruge resursele tehnice centralizat, astfel încât să nu fie posibil să restaurați informațiile stocate și să le ștergeți.

14.7. Ștergerea Datelor cu caracter personal este înregistrată (documentată) prin pregătirea unui act privind distrugerea Datelor cu caracter personal în caz de necesitate, prin faptul că nu permite includerea în actul relevant a informațiilor despre Datele cu caracter personal relevante care au fost distruse.

15. GESTIONAREA ȘI ÎNREGISTRAREA INCIDENTELOR DE SECURITATE

15.1. Persoana implicată în prelucrarea Datelor cu caracter personal care a găsit o amenințare notifică imediat Persoana Responsabilă și specialistul în domeniul protecției datelor al Companiei de orice amenințare referitoare la prelucrarea Datelor cu caracter personal, inclusiv cele descrise mai jos, utilizând numărul de telefon stabilit de Companie în acest scop și/sau adresa de email:

- dacă s-a descoperit o amenințare la adresa resurselor tehnice, inclusiv a resurselor IT (cum ar fi, întreruperea alimentării cu energie electrică, prezența lichidelor sau a particulelor, daune provocate de impactul fizic, incendiu sau inundație, pierderea sau furtul computerelor și alte mijloace tehnice etc.);

- dacă s-a descoperit o amenințare la adresa resurselor informaționale (de exemplu, Părțile Terțe au aflat parola de acces, s-a constat accesul neautorizat la Datele cu caracter personale, inclusiv pierderea suporturilor de informații USB, CD-uri, precum și trimiterea unui email ce conține Date cu caracter personal au fost găsite date către destinatari neintenționați, întreruperi în funcționarea Sistemului Informatic, ștergerea neautorizată sau corectarea Datelor cu caracter personal;

- dacă a fost găsit vreun tip de amenințare la adresa Datelor cu caracter personal în format de hârtie (cum ar fi, umiditate prea ridicată în locație, nefuncționarea lacătului unui dulap sau a ușilor din locație, nefuncționarea alarmei, accesul părților terțe la documente, pierderea documentelor etc.).

15.2. În cazul unei amenințări, Persoana implicată în prelucrarea Datelor cu caracter personal este obligată să asigure securitatea Sistemului Informatic în limita competențelor și autorizației sale, până la sosirea Persoanei Responsabile.

15.3. La primirea informațiilor despre apariția unui Incident de Securitate, persoana responsabilă de investigarea Incidentului de Securitate realizează următoarele acțiuni:

- evaluează care persoane din Companie ar trebui să fie notificate cu privire la eventualul Incident de Securitate, pentru a limita imediat impactul Incidentului de Securitate, pentru a minimiza consecințele, pentru a pune capăt Incidentului de Securitate, pentru a preveni repetarea Incidentului de Securitate;

- evaluează măsurile care urmează să fie puse în aplicare pentru a pune capăt Incidentului de Securitate (în cazul în care acesta nu s-a încheiat), pentru a limita impactul negativ al Incidentului de Securitate asupra Persoanei Vizate, pentru a minimiza eventualele pierderi și pentru a începe imediat punerea în aplicare a acestora;

- evaluează dacă este necesar să se notifice Incidentul de Securitate poliției (dacă acesta are caracteristicile unei infracțiuni) sau autorităților abilitate de lege;

- evaluează riscul cauzat de Incidentul de Securitate față de viața privată a persoanelor fizice prin evaluarea următoarelor aspecte:

  a) Au fost afectate Datele cu caracter personal în cadrul Incidentului de Securitate?
  b) Ce Date cu caracter personal au fost afectate?

c) Cât de sensibile sunt datele implicate în Incidentul de Securitate, acestea sunt date din Categoria Specială?
d) Care sunt persoanele care pot fi/sunt afectate în rezultatul Incidentului de Securitate, inclusiv numărul și categoriile de persoane afectate?
e) Cum și de ce a apărut Incidentul de Securitate?
f) Dacă datele au fost pierdute sau furate, poate Partea Terță să afle ceva despre persoana respectivă din datele relevante?
g) Care va fi impactul/consecințele Incidentului de Securitate asupra persoanelor implicate, inclusiv siguranța fizică a acestor persoane ar putea fi amenințată, pierderile materiale cauzate, deteriorarea reputației cauzate sau daunele morale cauzate?
h) Dacă datele au fost pierdute sau furate, datele au fost anonimizate, codificate, protejate cu o parolă sau protejate în alt mod?
i) Dacă datele ar fi fost furate sau pierdute, ar putea fi folosite în scopuri criminale?
j) Care va fi impactul/consecințele Incidentelor de Securitate asupra Companiei, inclusiv, dacă ar putea fi amenințate securitatea Companiei și/sau a Persoanei Vizate, ar putea provoca daune materiale (sancțiuni ale autorităților administrative, solicitări din partea Persoanei Vizate, daune ale reputației)?
k) Care sunt identitățile și persoanele de contact ale Persoanei Vizate afectate de Incidentul de Securitate pentru a putea să le contacteze dacă este cazul?

15.4. Operatorul de date cu caracter personal informează în scris Centrul Național pentru Protecția Datelor cu Caracter Personal despre incidentele de securitate constatate.

15.5. Notificarea Incidentului de Securitate Autorității de Supraveghere trebuie să conțină următoarele informații:

- informații despre Incidentul de Securitate și o scurtă descriere a Incidentului de Securitate;
- categoriile de Persoane Vizate implicate în Incidentul de Securitate, numărul aproximativ de Persoane Vizate afectate (domeniul de aplicare al Datelor cu caracter personal afectate);

- numele, prenumele și datele de contact al specialistului în domeniul protecției datelor sau o trimitere la un alt contact de la care Persoana Vizată ar putea obține informații suplimentare;
- Consecințele cauzate de un incident de securitate sau eventualele consecințe ale unui incident de securitate;
- Măsurile luate sau planificate de Companie pentru a atenua posibilele consecințe negative ale unui Incident de Securitate și pentru a nu permite astfel de Incidente de Securitate pe viitor;
- Alte informații, dacă acest lucru este prevăzut de legislația aplicabilă în vigoare în cazul unei notificări speciale, precum și alte informații considerate ca fiind necesare de către Companie.
- Persoana responsabilă de înregistrarea Incidentelor de Securitate evaluează fiecare notificare primită referitoare la un Incident de Securitate și, în cazul în care acest incident ar trebui să fie considerat ca fiind o încălcare a protecției Datelor cu caracter personal și poate cauza un risc ridicat pentru drepturile și libertățile persoanelor fizice, Persoana Responsabilă notifică Persoana Vizată implicată în Incidentul de Securitate al Incidentului de Securitate.

16. SUPRAVEGHERE VIDEO

16.1. Operatorul folosește un sistem de supraveghere video în limita parametrilor admisibili.

16.2. Intimitate: Se subînțelege și se acceptă că există o așteptare legitimă a unui anumit grad de intimitate a salariaților la locul de muncă, dar acest drept trebuie să fie echilibrat cu drepturile și interesele legitime ale Operatorului, în special dreptul de a-și administra eficient activitatea și dreptul de a se proteja de răspunderea față de terți pe care membrii colectivului o pot atrage.

17. MARCAREA DOCUMENTELOR

17.1. 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 conform Anexei 2.

18. RESPONSABILITATEA PENTRU ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL PRECUM ȘI A INFORMAȚIILOR CU ACCESIBILITATE LIMITATĂ

18.1. Operatorul de date cu caracter personal, persoana împuternicită de operator, persoanele terțe după caz, semnatari a anexei nr. 1, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 74^1 Cod contravențional) și penală (art. 177, 178, 180 Cod penal).

19. DISPOZIȚII FINALE

19.1. Prezenta Politică de securitate se completează cu prevederile legislației în vigoare.

19.2. Modificarea și completarea prezentei Politici de Securitate se face în modul stabilit pentru aprobarea acesteia.

19.3. Conținutul Politicii de securitate este revăzut și actualizat anual, pentru a reflecta orice modificări la cerințele de activității Operatorului, riscurile IT sau amenințările importante față de Sistemele Informaționale.

Anexa 1

la Politica de Securitate
a prelucrării Datelor cu Caracter
Personal
în cadrul activității „NEW POST
INTERNATIONAL" SRL

CATEGORIILE
de date cu caracter personal

1. Datele cu caracter personal, care direct sau indirect identifică o persoană fizică, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale, se împart în două categorii: obișnuite și speciale.

2.Categoria obișnuită o constituie informația care dezvăluie:
1) numele și prenumele;
2) sexul;
3) data și locul nașterii;
4) cetățenia;
5) IDNP;
6) imaginea;
8) situația familială;
9) situația militară;
10) datele personale ale membrilor de familie;
11) datele din permisul de conducere;
12) datele din certificatul de înmatriculare;
13) situația economică și financiară;
14) datele privind bunurile deținute;
15) datele bancare;
17) semnătura;
18) datele din actele de stare civilă;
19) numărul dosarului de pensie;
20) codul personal de asigurării sociale (CPAS);
21) codul asigurării medicale (CPAM);
22) numărul de telefon/fax;

23) numărul de telefon mobil;
24) adresa (domiciliului/reședinței);
25) adresa e-mail;
27) profesia și/sau locul de muncă;
28) formarea profesională - diplome - studii;

3. Categorii speciale de date cu caracter personal sînt datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancțiunile contravenționale. Operatorul nu prelucrează categorii speciale de date cu caracter personal.

Anexa 2

la Politica de Securitate
a prelucrării Datelor cu Caracter Personal
în cadrul activității „NEW POST INTERNATIONAL" SRL

1. **Model de marcaj de avertizare:**

   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.

2. **Model de marcaj supraveghere video:**

   În temeiul autorizării Centrului național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova, New Post International S.R.L., supraveghează zona video:

   Adresarea unei plângeri în privința prelucrării datelor cu caracter personal prin intermediul acestui sistem de evidență în adresa Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova, poate fi realizată doar după depunerea în prealabil a unei cereri operatorului de date cu caracter personal vizat.

Model: **Formular de consimțământ la transmiterea transfrontalieră a datelor cu caracter personal:**

În conformitate cu prevederile Legii 133 din 08.07.2011 privind protecția datelor cu caracter personal NEW POST INTERNATIONAL MLD SRL cu sediul în mun. Chișinău, bd. Ștefan cel Mare 65, of. 806, număr identificare de stat - cod fiscal 1014600029674 („**Companie**" „**Operator**") colectează și prelucrează unele date cu caracter personal care se refera la Dvs. Aceste date sunt orice informație referitoare la o persoană fizică identificată sau identificabilă.

Datele colectate sunt supuse transferului transfrontalier, fiind stocate pe serverele Operatorului care se află în Ucraina, fiind procesate de către New Post S.R.L. înregistrată în conformitate cu legislația Ucrainei, număr de înregistrare 31316718, al cărei sediu juridic se află pe adresa Ucraina, or. Kiev, șos. Stolicinoe nr 103, bl 1, et. 9, în calitate de Importator de date. Importatorul de date procesează datele în mărimea și condițiile stabilite de Acordul de transfer a datelor cu caracter personal semnat de către Operator și Importatorul de date.

În scopul corespunderii cu legislația în vigoare și în scopul unei bune colaborări dintre Companie și subiectul datelor cu caracter personal („**Subiect**"), acesta în baza prezentei își exprimă consimțământul liber, necondiționat, expres și conștient, și confirmă următoarele:

1. Prin prezenta, subiectul datelor cu caracter personal este de acord cu transmiterea transfrontalieră de către Companie a datelor sale personale, date care includ toate sau unele din următoarele categorii: numele, prenumele și patronimicul; Sexul Semnătura, Semnătura electronică, numărul personal de identificare de stat (IDNP); data și locul nașterii; cetățenia, datele din actele de stare civilă codul personal de asigurări medicale (CPAM) telefon mobil, adresă domiciliu/reședință telefon/ fax, email profesie, funcție formare profesională - diplome - studii situație familială datele membrilor de familie situație economică sau financiară Mărimea salariului brut, premii, sporuri, suplimente, stimulări, date din certificatul de concediu medical. date bancare imagine date din permisul de conducere sancțiuni disciplinare codul personal de asigurări sociale (CPAS) codul personal al asigurării medicale date din certificate de

înmatriculare locul de muncă, altele: certificat de concediu medical, mărimea salariului brut, premii, sporuri, stimulări, suplimente.

2. Subiectul datelor cu caracter personal prin prezenta acceptă și consimte că datele sale cu caracter personal vor fi transmise transfrontalier de către Companie pentru următoarele scopuri:
a) Executarea contractelor între Subiect și Companie;
b) Alte situații legate de relația contractuală pe care subiectul datelor o are sau o va avea cu Compania.

3. Subiectul datelor cu caracter personal consimte și acceptă că datele sale cu caracter personal pot fi transferate de către New Post S.R.L., în condițiile legii.

4. Subiectul datelor cu caracter personal prin prezenta consimte și acceptă precum că acest consimțământ este valabil pentru o perioadă de cinci ani, și poate fi reînnoit pentru perioade succesive de cinci ani. Consimțământul pentru procesarea datelor cu caracter personal poate fi retras în orice moment înainte de expirarea termenului, printr-o cerere scrisă, datată și semnată, depusă la sediul Operatorului.

5. Subiectul datelor cu caracter personal confirmă cunoașterea prevederilor Legii cu privire la protecția datelor cu caracter personal (nr. 133 din 08 iulie 2011), recunoscând că în legătură cu procesarea datelor sale de către Companie, are următoarele drepturi, cum e stabilit de lege:

- Dreptul la obținerea informațiilor privind identitatea operatorului sau a persoanei împuternicite de către operator, scopul prelucrării datelor colectate, precum și informații suplimentare referitoare la destinatarii datelor cu caracter personal;
- Dreptul de acces la datele sale cu caracter personal;
- Dreptul de intervenție asupra datelor cu caracter personal;
- Dreptul de opoziție;
- Dreptul de a nu fi supus unei decizii individuale;
- Accesul la justiție.

Pentru exercitarea acestor drepturi, subiectul datelor cu caracter personal este în drept să depună o cerere scrisă, datată și semnată, la sediul Operatorului.

6. Subiectul datelor cu caracter personal în conformitate cu art. 17 al Legii privind comerțul electronic (nr. 284 din 22 iulie 2004), consimte la procesarea datelor sale cu caracter personal și își exprimă consimțământul de a recepționa informație comercială în format electronic.

Consimțământul

Declar că am fost informat pe deplin cu privire la procesarea datelor cu caracter personal de către Companie și am citit în întregime, sunt de acord și accept toate clauzele Formularului de consimțământ cu privire la transmiterea frontalieră a datelor cu caracter personal. Mi-au fost aduse la cunoștință documentele Companiei privind securitatea datelor cu caracter personal, inclusiv ordinul Companiei privind protecția datelor cu caracter personal. Înțeleg că Compania poate primi, colecta, combina, organiza, utiliza, stoca, prelucra, transfera și dezvălui date cu caracter personal cu privire la persoana mea așa cum este prevăzut în prezentul Formular de Consimțământ. Declar că înțeleg și îmi exprim acordul cu privire la faptul că date cu caracter personal pot fi colectate, prelucrate, utilizate, transferate sau dezvăluite și că Compania își rezervă dreptul să realizeze aceste activități atunci când consideră necesar, iar date cu caracter personal pot fi transferate altor entități atât în interiorul cât și în afara Republicii Moldova, după cum este prevăzut mai sus în prezentul Formular de Consimțământ.

Nume:

Data **Semnătura**