REGULAMENTUL
"Paynet Services" S.R.L.
privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet, precum și a utilizatorilor participanți la programele de loialitate desfășurate cu suportul "Paynet Services" S.R.L.

1. DISPOZIŢII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet, precum și a utilizatorilor participanți la programele de loialitate desfășurate cu suportul "Paynet Services" S.R.L. (denumit în continuare "Regulament") este elaborat în vederea implementării în cadrul "Paynet Services" S.R.L. a prevederilor Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal și a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14 decembrie 2010, precum și întru respectarea prevederilor Politicii "Paynet Services" S.R.L. privind asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (Resursele umane interne și Datele personale ale utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet, precum și a utilizatorilor participanți la programele de loialitate desfășurate cu suportul "Paynet Services" S.R.L.).

1.2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale clienților "Paynet Services" S.R.L. în cadrul sistemului de evidență a utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet, precum și a utilizatorilor participanți la programele de loialitate desfășurate cu suportul "Paynet Services" S.R.L. (denumit în continuare "Sistem de evidență").

2. SCOPUL, CATEGORII DE DATE PRELUCRATE

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în Sistemul de evidență constă în asigurarea protecției datelor cu caracter personal în Sistemul de evidență a utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet, precum și a utilizatorilor participanți la programele de loialitate desfășurate cu suportul "Paynet Services" S.R.L. conform legislației în vigoare.

2.2. În cadrul Sistemului de evidență sînt prelucrate următoarele categorii de date cu caracter personal: nume, prenume, patronimic, data și anul nașterii, domiciliul, nr. și seria buletinului de identitate, condul de identificare (IDNP), nr. de telefon de la domiciliu, nr. de telefon mobil, semnătura, e-mail, situație economică sau financiară (soldul contului din sistemul de emitere a monedei electronice gestionat de "Paynet Services" S.R.L. și tranzacțiile efectuate), imagine, datele membrilor de familie, cetățenie (Notă: este intezisă fotocopierea anexei la buletinul de identitate în partea ce ține de participarea la alegeri).

2.3. Prelucrarea datelor cu caracter personal menționate va fi efectuată pentru realizarea următoarelor scopuri: ținerea evidenței utilizatorilor persoane fizice ale sistemului de plăți și emitere a monedei electronice Paynet și a operațiunilor financiare efectuate de aceste persoane, inclusiv recepționarea și eliberarea mijloacelor bănești în numerar, precum și evidența clienților persoane fizice participanți la programele de loialitate desfășurate cu suportul "Paynet Services" S.R.L. .

2.4. În cadrul prestării serviciilor de plată și de emitere a monedei electronice datele cu caracter personal al utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet pot fi transmise agenților "Paynet Services" S.R.L. (datele de identificare) în scopul recepționării sau eliberării mijloacelor financiare, acordării de facilități în cadrul programelor de loialitate desfășurate cu suportul "Paynet Services" S.R.L. și încheierea contractelor de aderare la serviiile prestate de "Paynet Services" S.R.L., precum și persoanelor în beneficiul cărora se vor efectua de către utilizatorii în cauză a tranzacțiilor financiare (nr. de telefon mobil (contul Paynet) și valoarea tranzacției), sub condiția că utilizatorii în cauză au permis "Paynet Services" S.R.L. în mod expres transmiterea acestor date prin încheierea Contractelor-cadru și a Cererii de aderare la sistemul Paynet, și

persoanele cărora li se vor transmite datele cu caracter personal vor asigura nivelul de protecție a acestor date prevăzut de legislația în vigoare.

2.5. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență al a utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet în alte scopuri, decît, cele menționate mai sus, este interzisă.

3. LOCAŢIA ŞI DESCRIEREA SISTEMULUI DE EVIDENȚĂ

3.1. Datele cu caracter personal conținute în sistemul de evidență a utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet se prelucrează/stochează: în regim manual pe suport de hîrtie (Contractele și cererile utilizatorilor ce conțin datele lor caracter personal de identificare) ce se află în safeu și în format electronic (datele cu caracter personal de identificare ale utilizatorilor, nr. de telefon mobile (echivalente cu nr. Conturilor Paynet, soldul conturilor Paynet, tranzacțiile financiare efectuate) pe serverele, ce se află în încăperi cu acces limitat ce sunt dotate cu lacăte la ușă și sistem de securitate în regim real. În perioada cînd din încăperile în cauză lipsesc angajații ferestrele sunt închise. La intrarea în imobilul în care se află încăperile în care sunt stocate și prelucrate datele cu caracter personal sunt postați agenți de pază, care efectuează controlul vizitatorilor în vederea limitării accesului persoanelor străine. De asemenea, încăperile în cauză sunt asigurate cu sisteme de siguranță antiincendiare.

3.2. Încăperea în care sunt stocate și prelucrate datele cu caracter personal se află la sediul "Paynet Services" S.R.L. din bd. Decebal 6, mun. Chișinău.

3.3. În calitate de persoană responsabilă de implementarea şi monitorizarea respectării prevederilor Politicii "Paynet Services" S.R.L. privind asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal și a prezentului Regulament este desmnat **Consultantul serviciilor informationale** a "Paynet Services" S.R.L.. Cheile de la safeul în care sunt păstrate datele cu caracter personal stocate pe suport de hîrtie se vor afla la Consultantul serviciilor informationale a "Paynet Services" S.R.L..

4. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidență se efectuează pe perioada existenței relațiilor contractuale între "Paynet Services" S.R.L. și utilizatorii respectivi a serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet și/sau utlizatorii participanți la programele de loialitate desfășurate cu suportul "Paynet Services" S.R.L., iar după încetarea realțiilor contractuale fiind arhivate și păstrate conform prevederilor legislației în vigoare pentru o perioadă de 5 ani.

5. DREPTURILE PERSOANELOR VIZATE

5.1. "Paynet Services" S.R.L., în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.

5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaților la informațiile ce vizează datele cu caracter personal a utilizatorilor serviciilor de plată și emitere a monedei electronice din cadrul sistemului Paynet se efectuează prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii. Informațiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

5.5. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informaţiile solicitate apar şi alte persoane şi nu există

posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

6. MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ

6.1. În cadrul "Paynet Services" S.R.L. se efectuează administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces. Înainte de acordarea accesului fizic la sistemul informaţional de date cu caracter personal se verifică competenţele de acces.

6.2. Perimetrul de securitate se determină concret şi clar. Purtătorii de informaţii şi mijloacele de prelucrare a datelor cu caracter personal care conţin date personale sunt amplasate în locuri cu acces limitat pentru persoane străine. 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 "Paynet Services" S.R.L.. Purtătorii de informaţii şi mijloacele de prelucrare a datelor cu caracter personal scoase din încăperile aflate în perimetrul de securitate nu trebuie lăsate fără supraveghere în locuri publice.

6.3. În cadrul "Paynet Services" S.R.L. este asigurat controlul accesului fizic al vizitatorilor în încăperea unde este amplasat sistemul informaţional de date cu caracter personal. Vizitatorii sistemului informaţional de date cu caracter personal sunt însoţiţi de persoane împuternicite în asemenea scop, cu exercitarea în paralel a controlului asupra acțiunilor acestora.

6.4. În cadrul "Paynet Services" S.R.L. este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere. În cadrul "Paynet Services" S.R.L. este administrat 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 sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii "Paynet Services" S.R.L..

6.5. Cerințe speciale față de marcare**:** toate informațiile ieșite din Sistemul de evidență, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

Model: **Atenţie!** Documentul conţine date cu caracter personal, prelucrate în cadrul Sistemului de evidenţă a "Paynet Services" S.R.L. 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

7. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENȚĂ

7.1. În cadrul "Paynet Services" S.R.L. este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori. Toţi utilizatorii în cauză: Consultantul sisteme informaționale și tehnicienii suport informațional (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) dispun de un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului v-or fi încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă sau se suspendă de către "Paynet Services" S.R.L.. În caz de necesitate de serviciu se acordă acces la datele cu caracter personal următoarelor persoane: Administrator, Director executiv, jurisconsult, contabil.

7.2. Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator;
2) verificarea autenticităţii fiecărui utilizator;
3) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului;
4) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;

5) dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (inacţiune în perioada de maximum 2 luni).

7.3. În cadrul "Paynet Services" S.R.L. se respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:

1) păstrarea confidenţialităţii parolelor;

2) interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;

3) modificarea parolelor de fiecare dată când sânt prezente indiciile eventualei compromiteri a sistemului sau parolei;

4) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere;

5) modificarea parolelor peste intervale de maximum șase luni;

6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

7.4. În cadrul "Paynet Services" S.R.L. se folosesc identificatoare individuale pentru fiecare utilizator a sistemului informațional de date cu caracter personal şi parole individuale ale acestora pentru asigurarea posibilităţii de stabilire a responsabilităţii și este asigurată posibilitatea utilizatorilor dați de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. În cadrul "Paynet Services" S.R.L. se asigură blocarea accesului după trei tentative greşite de autentificare şi este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioada de un an) şi prevenirea folosirii repetate a acestora.

8. ADMINISTRAREA ACCESULUI UTILIZATORILOR LA SISTEMUL DE EVIDENȚĂ

8.1. În cadrul "Paynet Services" S.R.L. sunt implementate mecanisme de înregistrare şi evidenţă a persoanelor care au acces sau participă la operaţiunile de prelucrare a datelor cu caracter personal şi care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

8.2. În cadrul "Paynet Services" S.R.L. este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Sînt folosite mijloace automatizate de suport în scopul administrării conturilor de acces. Sînt 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 şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

8.3. Accesul la funcţiile de securitate ale sistemelor informaţionale de date cu caracter personal şi la datele acestora este acordat doar persoanelor responsabile indicate expres în prezentul Regulament și în Politica privind asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal a "Paynet Services" S.R.L..

8.4. Drepturile de acces ale utilizatorilor la sistemele informaţionale de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni) şi după oricare schimbare de statut al utilizatorului.

8.5. În cadrul Companiei se realizarea controlul fluxurilor informaţionale în procesul transmiterii acestora în interiorul şi în afara sistemelor informaţionale de date cu caracter personal.

8.6. Repartizarea obligaţiilor subiecţilor care asigură funcţionarea sistemelor informaţionale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competenţe corespunzătoare de acces, prin ordinul Administratorului sau Directorului executiv al "Paynet Services" S.R.L.. Utilizatorii sistemelor informaţionale de date cu caracter personal se învestesc doar cu acele drepturi/competenţe, care sînt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

8.7. Înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea sistemelor informaţionale de date cu caracter personal este controlată şi că folosirea neautorizată a acestora se urmăreşte în conformitate cu legislaţia.

8.8. Sesiunea de lucru în sistemul informaţional electronic, destinat prelucrării datelor cu caracter personal, se blochează (la solicitarea utilizatorului sau automat, după maximum 5 de minute de perioadă inactivă a

utilizatorului), fapt care face imposibil accesul de mai departe pînă în momentul cînd utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

8.9. În cadrul "Paynet Services" S.R.L. se efectuează controlul acţiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

8.10. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate, supuse monitorizării şi controlului. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de persoanele responsabile ale Companiei şi permisă doar utilizatorilor cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

9. AUDITUL SECURITĂŢII ÎN SISTEMELE DE EVIDENŢĂ

9.1. În cadrul "Paynet Services" S.R.L. se organizează generarea înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

9.2. Lista evenimentelor înregistrate de sistemul de audit a securităţii în sistemele informaţionale de date cu caracter personal:

1) Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:
   a) data şi timpul tentativei intrării/ieşirii;
   b) ID-ul utilizatorului;
   c) rezultatul tentativei de intrare/ieşire – pozitivă sau negativă.

2) Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:
   a) data şi timpul tentativei de pornire;
   b) denumirea/identificatorul programului aplicativ sau procesului;
   c) ID-ul utilizatorului;
   d) rezultatul tentativei de pornire – pozitivă sau negativă.

3) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
   a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
   b) denumirea (identificatorul) aplicaţiei sau procesului;
   c) ID-ul utilizatorului;
   d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
   e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
   f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

4) 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.

5) 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;
   e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

9.3. În caz de deranjament al auditului securităţii în sistemele informaţionale de date cu caracter personal sau

completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este administratorul de rețea și întreprinse măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

9.4. În cadrul "Paynet Services" S.R.L. se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal, în scopul depistării activităţilor neobişnuite sau suspecte de utilizare a acestor sisteme informaţionale, cu întocmirea raportului referitor la cazurile depistării acestor activităţi, stocate în mijloacele electronice de calcul şi întreprinderea acţiunilor prestabilite în politica de securitate pentru astfel de cazuri.

9.5. Rezultatele auditului securităţii în sistemele informaţionale de date cu caracter personal, care reprezintă operaţiuni de prelucrare a datelor cu caracter personal şi mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidenţialităţii şi integrităţii acestora.

9.6. Durata stocării rezultatelor auditului securităţii în sistemele informaţionale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar în orice caz acest termen nu este mai mic de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

10. ASIGURAREA INTEGRITĂŢII INFORMAŢIILOR DIN SISTEMUL DE EVIDENȚĂ

10.1. În cadrul "Paynet Services" S.R.L. se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor soft-uri.

10.2. În cadrul "Paynet Services" S.R.L. se asigură protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus. Se asigură administrarea centralizată a mecanismelor de protecţie contra programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal.

10.3. În cadrul "Paynet Services" S.R.L. se utilizează tehnologii şi mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaţionale de date cu caracter personal şi constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaţionale.

10.4. În cadrul "Paynet Services" S.R.L. se asigură protecţia şi posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal şi informaţiei care conţine date cu caracter personal. Soft-urile destinate prelucrării datelor cu caracter personal şi informaţia care conţine date cu caracter personal, accesul la care se efectuează prin intermediul sistemelor de acces public, sînt securizate prin criptare.

10.5. În cadrul "Paynet Services" S.R.L. se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

11. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ

11.1. Personalul din cadrul "Paynet Services" S.R.L. care asigură exploatarea sistemelor informaţionale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

11.2. În cadrul "Paynet Services" S.R.L. este asigurat mecanismul de informare neîntîrziată a conducerii despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

11.3. Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent.

11.4. Anual, către 31 ianuarie, Serviciul Juridic al Companiei va prezenta Centrului de protecția a datelor cu caracter personal raportul generalizat despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal (doar în caz de aparție a unor astfel de incidente). În baza acestui raport, Centrul întreprinde măsurile ce se impun de Legea cu privire la protecţia datelor cu caracter personal.

11.5. In caz de incalcare a regimului de securitate a datelor personale a resurselor umane, persoana vinovată va purta responsabilitate în conformitate cu prevederile legislatei in vigoare, inclusiv raspunderea contraventionala si

penala.

12. DISPOZIŢII FINALE

12.1. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea "Paynet Services" S.R.L. periodic, însă cel puțin o dată în an, precum și la necesitate.

12.2. Prezentul Regulament se completează cu prevederile legislației în vigoare.

12.3. Regulamentul este adus la cunoştinţa angajaților contra semnăturii.

12.4. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.