**Aprobat**

**prin Ordinul nr. \_\_**

***\_\_ \_\_\_\_\_\_\_\_ 2019***

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*L.Ș.*

REGULAMENTUL

PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE

CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE

1. DISPOZIŢII GENERALE
   1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal (în continuare Regulament) este elaborat în vederea implementării în cadrul XXX (”Societatea„) - 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 art. 91 - 94 ale Codului muncii al Republicii Moldova.
   2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților Societății în cadrul sistemului de evidență resurse umane (denumit în continuare ”sistemul de evidență”).
2. SCOPUL
   1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență constă în asigurarea înregistrării informațiilor referitoare la recrutarea, angajarea, executarea clauzelor contractelor individuale de muncă, pensionarea salariaților, precum și a prezentării rapoartelor trimestriale şi anuale către instituţiile statului, conform legislației în vigoare.
   2. În cadrul sistemului de evidență sunt prelucrate următoarele categorii de date cu caracter personal:

* numele, prenumele, patronimicul;
* sexul;
* data și locul nașterii;
* semnătura;
* date din actele de stare civilă;
* CPAM;
* Telefon mobil;
* E-mail;
* Profesie, funcție;
* Formare profesională;
* Situația familială;
* Situație economică și financiară;
* Datele membrilor de familie:
* Cetățenia;
* Sancțiuni disciplinare;
* CPAS;
* Telefon/fax;
* Adresa (domiciliu/reședința);
* Loc de muncă;
* IDNP;
* Date bancare;
* Imagine:
* cetățenia;
* IDNP;
* imagine;
* mărime salariu brut, prime, stimulări, sporuri, suplimente, date din certificatul de concediu medical.
* după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.
  1. Prelucrarea datelor cu caracter personal menționate în cadrul sistemului de evidență resurse umane va fi efectuată pentru realizarea următoarelor scopuri:

1. Realizării activităților aferente recrutării;
2. Încheierea și executarea contractelor de muncă;
3. Furnizarea de beneficii;
4. Prezentarea la CNAM a evidenţei nominale a noilor angajaţi şi a celor concediaţi, format hârtie și format electronic
5. Administrarea resurselor umane la nivelul Societății (de ex., evaluare, training, proceduri disciplinare, plata salariilor, registre de personal, asigurarea securității și sănătății în muncă);
6. Desfășurarea de controale interne și externe de tip audit, cat si pentru cooperarea cu organizatiile profesionale;
7. Arhivare, îndeplinirea obligațiilor legale, apărare în caz de litigiu sau orice formă de neînțelegere între salariat și Societate.
   1. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către astfel încît să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămîne la păstrare primind statut de document de arhivă.

**III. LOCAŢIA ȘI DESCRIEREA SISTEMUL DE EVIDENȚĂ RESURSE UMANE**

* 1. Datele cu caracter personal conținute în sistemul de evidență în cadrul Societății se prelucrează/stochează pe suport de hîrtie.
  2. Prelucrarea informațiilor în sistemul de evidență pe suport de hîrtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sînt amplasate fizic în biroul XXX din sediul ZZZZ, Chișinău.

1. **DURATA DE STOCARE**
   1. Prelucrarea datelor cu caracter personal în sistemul de evidență resurse umane se efectuează pe perioada activității angajaților SRL XXX, valabilității contractelor individuale de muncă (din momentul semnării contractului până la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).
   2. Datele cu caracter personal a potențialilor salariați se preia din CV-ul transmis de către aceștia la adresa de e-mail a SC XXX SRL. După primirea CV-ului prin intermediul poștei electronice, acesta se tipărește pe suport de hârtie, iar de pe adresa de e-mail se șterge conținutul mesajului. Totodată, în cazul în care potențialii salariați nu au fost admiși la funcția vacantă din cadrulSC XXX SRL, atunci persoana responsabilă de sistemul de evidență a resurselor umane distruge CV-urile potențialilor angajați.
   3. La expirarea termenelor menționate în punctul 4.1., datele din sistemul de evidență resurse umane sînt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul dosarelor XXX aprobat prin Ordinul directorului XXX sau Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova, aprobat de Agenția Națională a Arhivelor nr.57 din 27.07.2016, ulterior fiind supuse distrugerii sau ștergerii, în funcție de suportul pe care au fost efectuate.

**V. DREPTURILE PERSOANELOR VIZATE**

**5.1.** Societatea 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 persoanelor vizate la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii Societății. Informațiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

**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 informațiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţămîntul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

**5.**6. Prelucrarea datelor cu caracter personal ale potențialilor salariați, precum și a salariaților se efectuează în conformitate cu art. 5 alin. (5) lit. a) și lit. b) ale Legii privind protecția datelor cu caracter personal, și anume: în cazul executării unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înaintea încheierii contractului, la cererea acestuia (în cazul încheierii contractului indivual de muncă) și în cazul îndeplinirii unei obligaţii care îi revine operatorului conform legii (în conformitate cu legislația muncii).

1. MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE

ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE

* 1. Măsurile generale de administrare a securităţii informaţionale
     1. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie care conţin date preluate din sistemul de evidență, aceştia se păstrează în safeuri care se încuie.
     2. La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la rețeaua electrică.
     3. Operatorul asigură securitatea punctelor de primire și expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.
     4. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidență este blocat împotriva vizualizării de către persoane neautorizate.
     5. Mijloacele de prelucrare a informațiilor preluate din sistemul de evidență sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
     6. Scoaterea şi introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență din/în perimetrul de securitate se înregistrează în registru.
  2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidență, se înfăptuiesc ţinînd cont de necesitatea asigurării confidenţialităţii și integrității acestora, prin protecţie în formă manuală.
  3. Cerințe speciale față de marcare: toate informațiile ieşite din sistemul de evidență, care conţin date cu caracter personal, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

**Model Atenţie!** Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, înregistrat în Registrul de evidenţă al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

* 1. Accesul în birourile Societății este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu card de acces (cartela de identificare). Cardul de acces nu poate fi transmis sau împrumutat nimănui.
  2. În cazul pierderii cardului de acces, acest fapt va fi raportat fără întârziere persoanelor responsabile cu gestionarea acestora iar cardul va fi blocat de îndată.
  3. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior,.
  4. Înainte de acordarea accesului fizic la sistemul de evidență, se verifică competenţele de acces.
  5. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.
  6. Perimetrul de securitate se consideră perimetrul birourilor în care este amplasat sistemul de evidență, fiind integre din punct de vedere fizic.
  7. Zilnic, se inspectează perimetrele de securitate al clădirii și al biroului, din punct de vedere fizic.
  8. Accesul persoanelor neautorizate în cadrul perimetrelor de securitate va fi chestionat pentru a evita accesul neautorizat și fiecare situație va fi raportată persoanelor responsabile cu acordarea drepturilor de acces și asigurarea securității.
  9. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.
  10. Amplasarea sistemului de evidență răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
  11. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidență , a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemul de evidență, inclusiv posibilitatea deconectării oricărui component TI.
  12. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaţionale.
  13. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidență. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

1. AUDITUL SECURITĂŢII ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE
   1. Se organizează generarea înregistrărilor de audit a securităţii în sistemul de evidență pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.
   2. Înregistrările de audit a securităţii sistemului de evidență în care sînt prelucrate date cu caracter personal, trebuie să conţină:

* numele şi prenumele utilizatorului;
* numele fişei accesate (pagina şi inscripţia din registru);
* numărul înregistrărilor efectuate;
* tipul de acces;
* data accesului (an, lună, zi);
* timpul (ora, minuta) şi durata accesului.
  1. Rezultatele auditului securităţii în sistemul de evidență (operaţiunile de prelucrare a informațiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidenţialităţii şi integrităţii acestora.
  2. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidență constituie 2 */doi/* ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

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

9.1. În conformitate cu art. 91 al Codului Muncii, angajatorul şi reprezentanţii lui sunt obligaţi să respecte următoarele cerinţe:

a) prelucrarea datelor personale ale salariatului poate fi efectuată exclusiv în scopul îndeplinirii prevederilor legislaţiei în vigoare, acordării de asistenţă la angajare, instruirii şi avansării în serviciu, asigurării securităţii personale a salariatului, controlului volumului şi calităţii lucrului îndeplinit şi asigurării integrităţii bunurilor unităţii;

b) la determinarea volumului şi conţinutului datelor personale ale salariatului ce urmează a fi prelucrate, angajatorul este obligat să se conducă de legislaţia în vigoare;

c) toate datele personale urmează a fi preluate de la salariat sau din sursa indicată de acesta;

d) angajatorul nu este în drept să obţină şi să prelucreze date referitoare la convingerile politice şi religioase ale salariatului, precum şi la viaţa privată a acestuia. În cazurile prevăzute de lege, angajatorul poate cere şi prelucra date despre viaţa privată a salariatului numai cu acordul scris al acestuia;

e) angajatorul nu este în drept să obţină şi să prelucreze date privind apartenenţa salariatului la sindicate, asociaţii obşteşti şi religioase, partide şi alte organizaţii social-politice, cu excepţia cazurilor prevăzute de lege;

f) la adoptarea unei decizii care afectează interesele salariatului, angajatorul nu este în drept să se bazeze pe datele personale ale salariatului obţinute exclusiv în urma prelucrării automatizate sau pe cale electronică;

g) protecţia datelor personale ale salariatului contra utilizării ilegale sau pierderii este asigurată din contul angajatorului;

h) salariaţii şi reprezentanţii lor trebuie să fie familiarizaţi, sub semnătură, cu documentele vizând modul de prelucrare şi păstrare a datelor personale ale salariaţilor din unitate şi să fie informaţi despre drepturile şi obligaţiile lor în domeniul respectiv;

i) salariaţii nu trebuie să renunţe la drepturile lor privind păstrarea şi protecţia datelor personale;

j) angajatorii, salariaţii şi reprezentanţii lor trebuie să elaboreze în comun măsurile de protecţie a datelor personale ale salariaţilor.

9.2. Conform art. 92 al CM, la transmiterea datelor personale ale salariatului, angajatorul trebuie să respecte următoarele cerinţe:

a) să nu comunice unor terţi datele personale ale salariatului fără acordul scris al acestuia, cu excepţia cazurilor când acest lucru este necesar în scopul prevenirii unui pericol pentru viaţa sau sănătatea salariatului, precum şi a cazurilor prevăzute de lege;

b) să nu comunice datele personale ale salariatului în scopuri comerciale fără acordul scris al acestuia;

c) să prevină persoanele care primesc datele personale ale salariatului despre faptul că acestea pot fi utilizate doar în scopurile pentru care au fost comunicate şi să ceară persoanelor în cauză confirmarea în scris a respectării acestei reguli. Persoanele care primesc datele personale ale salariatului sunt obligate să respecte regimul de confidenţialitate, cu excepţia cazurilor prevăzute lege;

d) să permită accesul la datele personale ale salariatului doar persoanelor împuternicite în acest sens, care, la rândul lor, au dreptul să solicite numai datele personale necesare exercitării unor atribuţii concrete;

e) să nu solicite informaţii privind starea sănătăţii salariatului, cu excepţia datelor ce vizează capacitatea salariatului de a-şi îndeplini obligaţiile de muncă;

f) să transmită reprezentanţilor salariaţilor datele personale ale salariatului în modul prevăzut de prezentul cod şi să limiteze această informaţie numai la acele date personale care sunt necesare exercitării de către reprezentanţii respectivi a atribuţiilor lor.

9.3. Conform art. 93 al CM, în scopul asigurării protecţiei datelor sale personale care se păstrează la angajator, salariatul are dreptul:

a) de a primi informaţia deplină despre datele sale personale şi modul de prelucrare a acestora;

b) de a avea acces liber şi gratuit la datele sale personale, inclusiv dreptul la copie de pe orice act juridic care conţine datele sale personale, cu excepţia cazurilor prevăzute de legislaţia în vigoare;

c) de a-şi desemna reprezentanţii pentru protecţia datelor sale personale;

d) de a avea acces la informaţia cu caracter medical ce-l vizează, inclusiv prin intermediul lucrătorului medical, la alegerea sa;

e) de a cere excluderea sau rectificarea datelor personale incorecte şi/sau incomplete, precum şi a datelor prelucrate cu încălcarea cerinţelor prezentului cod. În cazul în care angajatorul refuză să excludă sau să rectifice datele personale incorecte, salariatul este în drept să notifice în scris angajatorului dezacordul său motivat;

f) de a ataca în instanţa de judecată orice acţiuni sau inacţiuni ilegale ale angajatorului admise la obţinerea, păstrarea, prelucrarea şi protecţia datelor personale ale salariatului

1. DISPOZIŢII FINALE
   1. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea Societății periodic, însă cel puțin o dată în an, precum și la necesitate.
   2. Prezentul Regulament se completează cu prevederile legislației în vigoare.
   3. Regulamentul este adus la cunoştinţa angajaților prin comunicare directă sau prin publicarea pe pagina de Internet a Societății.
   4. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.