PROTECŢIA PERSOANELOR CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL ŞI LIBERA CIRCULAŢIE A ACESTOR DATE LA NIVELUL **SUN GARDEN MANAGEMENT S.C.S.**

SCOPUL

Scopul acestei proceduri este de a garanta şi proteja drepturile şi libertăţile fundamentale ale persoanelor fizice, în special a dreptului la viaţa intimă, familială şi privată, cu privire la prelucrarea datelor cu caracter personal.

I. REGULI GENERALE

Art. 1. Prezenta procedură stabilește măsuri tehnice şi organizatorice pentru îndeplinirea obligațiilor referitoare la securitatea şi controlul sistemelor informatice, în vederea asigurării confidențialității datelor şi informațiilor precum şi pentru păstrarea în siguranţă a acestora, în cadrul activității curente executate de angajații SUN GARDEN MANAGEMENT S.C.S.. Prin cerințe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri şi politici de securitate prin care să se asigure nivelul minim de securitate prevăzut în art. 20 din Legea nr. 677/2001, în conformitate cu cerințele minime de securitate a prelucrărilor de date cu caracter personal, aprobate prin Ordinul 52 din 18 aprilie 2002 ale Avocatului Poporului.

Art. 2. SUN GARDEN MANAGEMENT S.C.S. a adoptat măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. În acest sens au fost desemnate, la nivelul SUN GARDEN MANAGEMENT, persoane responsabile cu respectarea dispozițiilor Legii nr.677/2001.

Art. 3 SUN GARDEN MANAGEMENT S.C.S a luat măsuri de stocare în siguranță a informațiilor, astfel încât să fie asigurat un nivel adecvat de protecție şi securitate, în sensul Legii 677/2001.

Art.4. Pentru îndeplinirea prevederilor legale aferente şi în vederea satisfacerii cerinţelor păstrării în siguranţă a datelor şi informaţiilor, instituţia a elaborat şi implementat măsuri organizatorice şi tehnice orientate pe anumite direcţii de acţiune: - Identificarea şi autentificarea utilizatorului - Tipul de acces - Colectarea datelor - Execuţia copiilor de siguranţă - Computerele şi terminalele de acces - Fişierele de acces și Instruirea personalului.

II. PROCEDURI SPECIFICE

Art. 5. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI

Prin utilizator se înţelege orice persoană care acţionează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

Utilizatorii, pentru a obține acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea în cadrul SUN GARDEN MANAGEMENT S.C.S se face prin introducerea codului de identificare de la tastatură (un şir de caractere).

Fiecare utilizator are propriul său cod de identificare. Niciodată nu este alocat acelaşi cod de indentificare mai multor utilizatori. Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată sunt dezactivate şi distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate şi distruse este stabilită prin proceduri interne de operator.

Orice cont de utilizator este însoţit de o modalitate de autentificare. Autentificarea se face prin introducerea unei parole. Parolele sunt şiruri de caractere, adecvate din punct de vedere al securităţii ca lungime şi compoziţie. La introducerea parolelor acestea nu sunt afişate în clar pe monitor. Parolele sunt schimbate periodic în funcţie de politicile de securitate ale operatorului. Schimbarea periodică a parolelor se face numai de către utilizatori autorizaţi de operator. Operatorul are implementate un sistem informaţional care refuză automat accesul unui utilizator după 3 introduceri greşite ale parolei.

Orice utilizator care primeşte un cod de identificare şi un mijloc de autentificare este obligat prin fişa postului să păstreze confidenţialitatea acestora şi să răspundă în acest sens în faţa operatorului. Este stabilită o procedură proprie de administrare şi gestionare a conturilor de utilizator. Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se face numai pe baza unei liste aprobate de conducerea instituției.

Art. 6. TIPUL DE ACCES

Utilizatorii pot accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu. Pentru aceasta sunt stabile tipurile de acces după funcţionalitate (administrare, introducere, prelucrare, salvare etc.) şi după acţiuni aplicate asupra datelor cu caracter personal (scriere, citire, ştergere), precum şi procedurile privind aceste tipuri de acces.

Programatorii sistemelor de prelucrare a datelor cu caracter personal nu au acces la datele cu caracter personal.

Operatorul permite accesul programatorilor la datele cu caracter personal numai după ce acestea au fost transformate în date anonime.

Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea unor cazuri excepţionale.

Alte măsuri specifice implementate de control al acesulului sunt: - în spaţiile destinate desfăşurării activităţii instituţiei sunt instalate sisteme de alarmă antiefracţie ; - în spaţiul aferent intrării în cadrul instituţiei sunt instalate sisteme de supraveghere video; și monitorizarea şi intervenţia în caz de alarmă este asigurată de o firmă de protecţie şi pază.

Art. 7. COLECTAREA DATELOR

Operatorul desemnează utilizatori autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional.

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizaţi desemnaţi de operator.

Operatorul a luat măsuri pentru ca sistemul informaţional să înregistreze cine a făcut modificarea, data și ora modificării. Pentru o mai bună administrare operatorul are implementate măsuri ca sistemul informaţional să menţină datele şterse sau modificate.

Art. 8. EXECUŢIA COPIILOR DE SIGURANŢĂ

Operatorul stabileşte intervalul de timp la care se vor executa copiile de siguranţă ale bazelor de date cu caracter personal, precum şi ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranţă sunt numiţi de operator, într-un număr restrâns. Copiile de siguranţă se vor stoca în alte camere, în fişete metalice.

Operatorul a luat măsuri ca accesul la copiile de siguranţă să fie monitorizat. Se generează zilnic de către sistemul informatic, în mod automat, un back-up pentru o eventuală recuperare a datelor, în cazul distrugerii sau disfuncţionalităţii sistemelor informatice.

Art. 9. COMPUTERELE ŞI TERMINALELE DE ACCES

Computerele şi alte terminale de acces sunt instalate în încăperi cu acces restricţionat. Unde nu pot fi asigurate aceste condiţii, computerele sunt instalate în încăperi care se pot încuia. Dacă pe ecran apar date cu caracter personal asupra cărora nu se acţionează o perioadă dată, stabilită de operator, sesiunea de lucru se închide automat.

Mărimea acestei perioade se determină în funcţie de operaţiile care trebuie executate. Terminalele de acces folosite în relaţia cu publicul, pe care apar date cu caracter personal, vor fi poziţionate astfel încât să nu poată fi văzute de public şi după o perioadă scurtă, stabilită de operator, în care nu se acţionează asupra lor, acestea trebuie ascunse.

Serverele care găzduiesc bazele de date pot fi accesate doar în mod controlat, pe baza de drepturi de acces; nu pot fi accesate din afara reţelei ANPC. Nu este permisă scoaterea din instituţie a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD), decât cu aprobare prealabilă din partea conducerii instituţiei.

Art. 10. FIŞIERELE DE ACCES

Operatorul ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fişier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator.

Informaţiile înregistrate în fişierul de acces sau în registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fişierului accesat (fişei);
- numărul înregistrărilor efectuate;
- tipul de acces;
- codul operaţiei executate sau programul folosit;
- data accesului (an, lună, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrările automate aceste informaţii vor fi stocate într-un fişier de acces general sau în fişiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

Operatorul este obligat să păstreze fişierele de acces cel puţin 2 ani, pentru a fi folosite ca probe în cazul unor investigaţii. Dacă investigaţiile se prelungesc, aceste fişiere se vor păstra atât timp cât se va considera necesar.

Fişierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancţiuni sau a sesizării organelor competente.

Art. 11. INSTRUIREA PERSONALULUI

Operatorul face informarea personalului cu privire la prevederile Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, la cerinţele minime de securitate a prelucrărilor de date cu caracter personal, precum şi cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii.

Utilizatorii care au acces la date cu caracter personal sunt instruiţi de către operator asupra confidenţialităţii acestora şi sunt avertizaţi prin mesaje care vor apărea pe monitoare în timpul activităţii.

Art. 12. FOLOSIREA COMPUTERELOR

Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva virusilor informatici) operatorul va lua măsuri care vor consta în:

- interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;
- informarea utilizatorilor în privinţa pericolului privind viruşii informatici;
- implementarea unor sisteme automate de devirusare şi de securitate a sistemelor informaţice;
- dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afişate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.

Art. 13. IMPRIMAREA DATELOR

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru această operaţiune de către operator.

III. REGULI SPECIALE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

Art. 14. În scopul protejării datelor cu caracter personal, s-au luat următoarele măsuri:

Cerinţele minime de securitate acoperă urmatoarele categorii de prelucrări de date cu caracter personal şi se referă la:

1. Prelucrări automate de date cu caracter personal

Accesul utilizatorilor la bazele de date ce conţin date cu caracter personal se va efectua prin coduri personale de acces (nume de logare, nume de utilizator).

Codurile de acces sunt protejate prin metode de autentificare (parole, certificate).

Codurile de acces (conturi utilizator) sunt alocate individual pentru fiecare utilizator.

Conturile de utilizator nefolosite o perioada 30 zile sunt sterse sau dezactivate permanent.

Codurile de acces se vor dezactiva automat după un număr de 3 încercari de logare nereuşite.

Codurile de acces vor permite doar nivelul minim de acces la datele cu caracter personal ce sunt necesare pentru îndeplinirea atribuţiilor de serviciu.

Computerele şi terminale de acces sunt instalate în incaperi cu acces restricţionat.

Documentele care conţin date cu caracter personal sunt ţinute în fişete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare.

Documentele care conţin date cu caracter personal, folosite pentru realizarea anumitor operaţiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora.

Prelucrarea datelor cu caracter personal se va efectua numai de către utilizatorii desemnaţi de instituţie prin proceduri interne.

IV. CATEGORII DE PERSOANE ȘI SCOPUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Art.15. SUN GARDEN MANAGEMENT S.C.S, prelucrează datele cu caracter personal ale angajaților societății, în scopul întocmirii situațiilor lunare care au strictă legătura cu

salarizarea și tot ceea ce decurge din aceasta, strict cu respectarea prevederilor legale, în vederea îndeplinirii obligațiilor față de autoritățile statului, și în interesul salariaților.

Art.16. UTILIZATORII AU URMĂTOARELE OBLIGAȚII SPECIFICE:

a) să cunoască şi să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum şi ale prezentei proceduri;
b) să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condițiile legii, cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute şi consecinţele refuzului de a le pune la dispoziţie, drepturile prevăzute de lege, în special drepturile de acces, de intervenţie asupra datelor şi de opoziţie, condiţiile în care pot fi exercitate aceste drepturi;
c) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu şi să acorde sprijin conducătorului operatorului pentru realizarea activităţilor specifice ale acestuia;
d) să păstreze confidenţialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;
e) să respecte măsurile de securitate, precum şi celelalte reguli stabilite de operator;
f) să informeze de îndată conducerea instituţiei despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situaţie în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoştinţă.

Art.17. Dreptul de opoziție al persoanelor a căror date personale sunt colectate şi/ sau prelucrate

(1) Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate şi legitime legate de situaţia sa particulară, ca date care o vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care există dispoziţii legale contrare. În caz de opoziţie justificată prelucrarea nu mai poate viza datele în cauză.

(2) În vederea exercitării drepturilor prevăzute la alin. (1) persoana vizată va înainta societății o cerere întocmită în formă scrisă, înregistrată la Registratură şi semnată. În cerere, solicitantul poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal.

(3) Societatea este obligata să comunice persoanei vizate măsurile luate în temeiul alin. (1) precum şi, dacă este cazul, numele terţului căruia i-au fost dezvăluite datele cu caracter personal referitoare la persoana vizată, în termen de 15 zile de la data primirii cererii

V. COMUNICAREA DATELOR CU CARACTER PERSONAL

Art.18. Datele cu caracter personal se pot comunica între departamentele societatii, precum si intre acestea si alte instituţii ori organisme publice sau entităţi de drept public sau privat în una dintre următoarele situaţii:

a) dacă persoana vizată şi-a dat consimţământul expres şi neechivoc pentru prelucrarea/comunicarea datelor sale;
b) fără consimţământul persoanei vizate în cazurile prevăzute de lege.