

Procedură privind protecția și securitatea sistemelor informatice
unde se stochează și prelucrează date cu caracter personal
în cadrul firmei SOLAR POWER MANGEMENT SRL

CONȚINUTUL PROCEDURII

SCOP: Această procedură stabilește:

1. Un set unitar de reguli care reglementează protecția și securitatea sistemelor informatice unde se stochează și se prelucrează date în cadrul **SOLAR POWER MANGEMENT SRL** în scopul asigurării, respectând în același timp obligațiile ce revin **SOLAR POWER MANGEMENT SRL** și măsurile de securitate adoptate pentru protecția datelor cu caracter personal, protejarea vieții private, a intereselor legitime și garantarea drepturilor fundamentale ale persoanelor vizate.
2. Responsabilitățile privind protecția și securitatea sistemelor informatice unde se stochează și se prelucrează date, precum și cele privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.

Procedura privind protecția și securitatea sistemelor informatice unde se stochează și prelucrează date cu caracter personal prezintă măsurile de protecție luate de **SOLAR POWER MANGEMENT SRL** pentru a proteja datele cu caracter personal, viața privată și alte drepturi fundamentale și interese legitime ale persoanelor ale căror date au ajuns în posesia firmei **SOLAR POWER MANGEMENT SRL**.

DOMENIUL: Procedura se aplica în cadrul activității de prelucrare protective și stocare a datelor personale. Politica se aplică, corespunzător competențelor, de către:

- personalul desemnat din cadrul Structurii de Tehnologia Informației;
- structura responsabilă cu protecția datelor personale;
- personalul extern care asigură mentenanța infrastructurii IT din cadrul firmei;
- angajaților **SOLAR POWER MANGEMENT SRL**.

TERMENI ȘI DEFINIȚII:

ANSPDCP= Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;

Codul numeric personal (CNP)= un număr semnificativ care individualizează în mod unic o persoană fizică, constituind un instrument de verificare a stării civile a acesteia și de identificare în anumite sisteme informatice de către persoanele autorizate;

Date cu caracter personal= orice informații referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulți factori specifici identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

Date cu caracter personal cu funcție de identificare de aplicabilitate generală (date cu caracter special) = numere prin care se identifică o persoană fizică în anumite sisteme de evidență și care au aplicabilitate generală, cum ar fi: codul numeric personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate;

Date anonime - date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă;

Operator - Persoana fizică sau juridică, autoritatea publică, agenția sau al organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

Persoană împuternicită de către operator - o persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului;

Responsabilul cu protecția datelor - DPO – persoana desemnată cu:

- Informarea și consilierea operatorului precum și a angajaților cu privire la obligațiile care le revin în referitoare la protecția datelor;
- Monitorizarea respectării regulamentului GDPR și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv acțiunile de sensibilizare și de formare a personalului;
- Furnizarea de consiliere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
- Cooperarea cu autoritatea de supraveghere;
- Asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare.

Utilizator - orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal;

Prelucrarea datelor cu caracter personal - orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terți prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

Stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, respectând în același timp protecția datelor cu caracter personal „începând cu momentul conceperii și în mod implicit” (by design and by default);

Pseudonimizarea datelor - prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate;

Funcție hash (hash function) - reprezintă un algoritm matematic criptografic care generează un checksum (rezumat criptografic) unic pentru fiecare mesaj. Acest checksum se numește *message diggest, diggest sau hash*.

1. CONDIȚII DE LEGITIMITATE

SOLAR POWER MANGEMENT SRL prelucrează datele cu caracter personal înregistrate în sistemele informatice IT ale firmei, asigură protecția și securitatea sistemelor informatice unde se stochează și prelucrează date cu caracter personal respectând prevederile legale în domeniu.

1.1 Referințe normative:

- a) Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare;
- b) Ordinul nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal;
- c) Ordinul Avocatului Poporului nr. 52 din 18/04/2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal;
- d) Decizia ANSPDCP nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video;
- e) Decizia ANSPDCP nr. 132 din 20/12/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală;
- i) Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.**

1.2 Transparentă

Procedura privind protecția și securitatea sistemelor informatice unde se stochează și prelucrează date cu caracter personal este disponibilă ca anexă a Regulamentului de Ordine Interioară **SOLAR POWER MANGEMENT SRL**.

1.3 Revizuiți periodice

O revizuire periodică va fi întreprinsă anual sau ori de câte ori apar modificări legislative, de către structurile responsabile cu asigurarea securității și va reanaliza:

- îndeplinirea scopului declarant;
- posibile îmbunătățiri ale **procedurii privind protecția și securitatea sistemelor informatice unde se stochează și prelucrează date cu caracter personal**.

2. Reguli Generale

Prin cerințe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri și politici de securitate prin care să se asigure nivelul minim de securitate prevăzut în art. 20 din Legea nr. 677/2001 și luând în considerare cerințele din legislația națională, deciziile ANSPDCP în acest domeniu și Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

SOLAR POWER MANGEMENT SRL a adoptat măsuri tehnice și organizatorice adecvate pentru protecția și securitatea sistemelor informatice unde se stochează și se prelucrează date personale, precum și măsuri tehnice și organizatorice adecvate necesare pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat la sistemele informatice unde se stochează datele personale. În acest sens au fost desemnate, la nivelul **SOLAR POWER MANGEMENT SRL**, persoane responsabile cu respectarea dispozițiilor Legii nr.677/2001.

SOLAR POWER MANGEMENT SRL a luat măsuri de stocare în siguranță a informațiilor privind date cu caracter personal, astfel încât să fie asigurat un nivel adecvat de protecție și securitate, în sensul Legii 677/2001 al deciziilor ANSPDCP în acest domeniu și Regulamentul (UE) 2016/679.

3. Accesul protejat la sistemele informatice unde se stochează și prelucrează date cu caracter personal în cadrul SOLAR POWER MANGEMENT SRL

3.1. PROCEDURI SPECIFICE

3.1.1. Accesul la serverele din cadrul firmei SOLAR POWER MANGEMENT SRL

În spațiile destinate desfășurării activității instituției sunt instalate sisteme de alarmă antiefracție:

- în spațiul aferent intrării în cadrul instituției și în holurile de acces este instalat un sistem de supraveghere video;
- monitorizarea și intervenția în caz de alarmă este asigurată de o firmă de protecție și pază;
- serverele care găzduiesc date cu caracter personal pot fi accesate doar în mod controlat, pe baza de drepturi de acces, conform politicilor de securitate ale grupului și adoptate de **SOLAR POWER MANGEMENT SRL** ;
- accesul în camera serverelor care găzduiesc date cu caracter personal este restricționat printr-un sistem de control acces cu cartelă. Administratorul de sistem este persoana împuternicită să efectueze orice fel de schimbări hardware/software ale serverelor companiei. Orice fel de schimbare software/hardware pe serverele companiei, este precedată de un set de măsuri tehnice de backup a sistemelor pentru a asigura buna funcționalitate în ansamblu a întregului sistem informatic din cadrul companiei în cazul apariției unei defecțiuni majore a serverelor în timpul procedurilor de upgrade software/hardware. Compania **SOLAR POWER MANGEMENT SRL** asigură redundanță din punct de vedere al alimentării cu energie electrică a serverelor din companie, prin montarea de UPS-uri (surse de alimentare neîntreruptibile) performante care asigură o stabilitate în alimentarea cu energie electrică atât din punct de vedere al tensiunii și amperajului furnizat către servere cât și din punct de vedere al alimentării cu energie electrică în cazul unei defecțiuni în rețeaua de alimentare cu energie electrică pentru o perioadă de minim o 1 ora. În cazul depășirii acestei perioade de 1 oră, intră în acțiune procedura software tehnică automată de stingere controlată a serverelor pentru a evita orice pierdere de datelor stocate pe servere.

Nu este permisă scoaterea din instituție a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD) care conțin date cu caracter personal, decât cu aprobare prealabilă din partea conducerii instituției.

SOLAR POWER MANGEMENT SRL ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată.

3.1.2. Identificarea și autentificarea utilizatorului într-un sistem informatic în cadrul firmei SOLAR POWER MANGEMENT SRL

Pentru a căpăta acces la date cu caracter personal, utilizatorii trebuie să se autentifice în sistemele informatice ale **SOLAR POWER MANGEMENT SRL**. Autentificarea în cadrul sistemelor informatice ale **SOLAR POWER MANGEMENT SRL** se face prin introducerea credențialelor de autentificare unice și netransmisibile dobândite în urma procesului de înrolare și management al identității electronice, guvernat de politicile de securitate în vigoare.

Fiecare utilizator are propriul său cod de identificare (nume de utilizator). Niciodată nu este alocat același cod de indentificare mai multor utilizatori și acesta nu poate fi partajat de către mai multe persoane.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai mare de **1 an** sunt dezactivate și distruse după un control prealabil. Orice cont de utilizator este însoțit de o modalitate de autentificare, prin introducerea unei chei de autentificare precum o parolă, un certificat digital sau un răspuns generat de un token.

Parolele sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție. La introducerea parolelor acestea nu sunt afișate în clar pe monitor. Parolele sunt schimbate periodic conform politicilor de Securitate **SOLAR POWER MANGEMENT SRL**. Schimbarea periodică a parolelor se face numai de către utilizatori autorizați.

Sistemul informațional blochează automat accesul unui utilizator după un numar fix de introduceri greșite ale cheii de autentificare.

Cheia de autentificare (sau parola de acces) este o înșiruire de caractere, adecvate din punct de vedere al securității informatice ca lungime și compoziție.

Orice utilizator care primește un cod de identificare și un mijloc de autentificare este obligat prin fișa postului să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului.

Este stabilită o procedură proprie de administrare și gestionare a conturilor de utilizator. Sunt autorizați anumiți utilizatori pentru a revoca sau a suspenda un cod de identificare și autentificare, dacă utilizatorul acestora și-a dat demisia ori a fost concediat, și-a încheiat contractul, a fost transferat la alt serviciu și noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată stabilită de entitate.

3.1.3. Tipul de acces

Utilizatorii trebuie sa acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu. Pentru aceasta trebuie sa fie stabilite tipurile de acces după funcționalitate (administrare, introducere, prelucrare, salvare

etc.) și după acțiuni aplicate asupra datelor cu caracter personal (scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces.

Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea incidentelor și a problemelor apărute în utilizarea sistemelor informatice.

Alte măsuri specifice implementate pentru controlul accesului, sunt:

- în spațiile destinate desfășurării activității instituției sunt instalate sisteme de alarmă antiefracție;
- în spațiul aferent intrării în cadrul instituției și în holurile de acces la etajele superioare sunt instalate sisteme de supraveghere video;
- monitorizarea și intervenția în caz de alarmă este asigurată de o firmă de protecție și pază.

3.1.4. Criptarea datelor în cadrul SOLAR POWER MANGEMENT SRL – metode specifice de criptare și de pseudonimizare a datelor cu caracter personal

În procesul de securizare și protecție a sistemelor informatice unde se stochează și se prelucrează date personale, criptarea datelor folosind un algoritm de criptare, alături de toate celelalte măsuri de ordin tehnic și organizatoric în cadrul **SOLAR POWER MANGEMENT SRL**, protejează informațiile și datele cu caracter personal de accesul nedorit și de prelucrarea neautorizată și ilegală a datelor.

Păstrarea pe orice fel de suport hardware a datelor cu caracter personal culese în cadrul **SOLAR POWER MANGEMENT SRL**, respectă protecția datelor cu caracter personal începând cu momentul conceperii și în mod implicit (by design and by default).

Standardul de criptare folosit este **AES** (de la **Advanced Encryption Standard** – în limba engleză, Standard Avansat de Criptare), cunoscut și sub numele de Rijndael, este un algoritm standardizat pentru criptarea simetrică, pe blocuri. Datele de identificare sunt ținute separat într-un dulap securizat cu acces limitat, în cadrul **SOLAR POWER MANGEMENT SRL**, astfel încât să nu poată fi făcută legătura cu o persoană fizică. Pseudonimizarea nu anonimizează datele cu caracter personal, dar identificarea directă nu mai este posibilă. Riscurile asociate cu prelucrarea datelor sunt reduse, dar în același timp se menține utilitatea datelor. Modalitatea tehnică de pseudonimizare a datelor, folosită în cadrul **SOLAR POWER MANGEMENT SRL** este pseudonimizarea prin intermediul funcțiilor hash, folosite pentru a mapa date de orice dimensiune către coduri de dimensiuni fixe.

3.1.5. Execuția copiilor de siguranță

SOLAR POWER MANGEMENT SRL a stabilit intervalul de timp de **1 lună** la care se vor executa copiile de siguranță ale bazelor de date ce conțin date cu caracter personal.

Utilizatorii care execută aceste copii de siguranță sunt numiți de **SOLAR POWER MANGEMENT SRL**, într-un număr restrâns.

Accesul la copiile de siguranță trebuie să fie monitorizat.

Sistemele care gestionează date cu caracter personal trebuie să fie protejate prin procesul de backup periodic împotriva pierderii, sau distrugerii datelor sau a sistemului informatic.

4. Protecția și securitatea sistemelor informatice unde se stochează date cu caracter personal

4.1. Măsurile de păstrare a confidențialității

După angajare în cadrul firmei **SOLAR POWER MANGEMENT SRL**, fiecare persoană nou angajată face un instructaj cu privire la procedurile existente în cadrul firmei și cu privire la Regulamentul de Ordine Interioară **SOLAR POWER MANGEMENT SRL**. După instructaj, fiecare persoană nou angajată semnează o declarație de confidențialitate.

Orice alt partener al firmei **SOLAR POWER MANGEMENT SRL** care vine în contact de orice fel cu serverele principale care asigură buna funcționalitate a sistemelor informatice din cadrul firmei **SOLAR POWER MANGEMENT SRL**, este obligat să semneze o declarație de confidențialitate.

4.2 Dezvăluirea datelor cu caracter personal

Orice activitate de dezvăluire a datelor personale către terți va fi documentată și supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, și pe de altă parte compatibilitatea dintre scopul în care se face comunicarea și scopul în care aceste date au fost colectate inițial pentru prelucrare (de securitate și control acces). În aceste cazuri va fi consultat și Responsabilul cu Protecția Datelor Personale. În cazuri excepționale, dar cu respectarea garanțiilor descrise mai sus, se poate acorda acces Comisiei Disciplinare, în cadrul unei anchete disciplinare, cu condiția ca informațiile să ajute la investigarea unei infracțiuni sau a unei abateri disciplinare de natură să prejudicieze drepturile și libertățile unei persoane. Orice încălcare a securității datelor personale colectate este indicată în Registrul de Investigații, iar Responsabilul cu Protecția Datelor Personale este informat în legătură cu acest lucru cât mai repede posibil.

4.3. GARANTAREA DREPTURILOR PERSOANEI VIZATE

SOLAR POWER MANGEMENT SRL garantează că asigură respectarea drepturilor ce revin persoanelor vizate, conform legii. Toate persoanele implicate în activitatea de colectare a datelor personale și cele responsabile de administrarea imaginilor filmate, și toate persoanele implicate în protecția și securitatea sistemelor informatice unde se stochează date personale, vor respecta **Procedura specifică de acces, prelucrare și protecție a datelor cu caracter personal** în cadrul firmei **SOLAR POWER MANGEMENT SRL**.

