Procedură de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal

CONŢINUTUL PROCEDURII

SCOP: Această procedură stabileşte:

1. Un set unitar de reguli care reglementează activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, conform legislatiei europene prin aplicarea Regulamentului nr. 679/2016;
2. Responsabilităţile privind activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal în cadrul **SOLAR POWER MANGEMENT SRL** , precum şi cele privind întocmirea, avizarea şi aprobarea documentelor aferente acestor activităţi.

Procedura de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal prezintă măsurile luate de **SOLAR POWER MANGEMENT SRL** pentru a proteja drepturile pe care le au persoanele fizice vizate de prelucrarea datelor cu caracter personal, conform legislatiei europene prin aplicarea Regulamentului nr. 679/2016 şi interesele legitime ale acestor persoane ale caror date au ajuns în posesia firmei **SOLAR POWER MANGEMENT SRL** .

DOMENIUL: Procedura se aplica în activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal. Procedura se aplică, corespunzător competenţelor, de către:

- personalul desemnat din cadrul Structurii de Tehnologia Informaţiei;
- structura responsabilă cu protecţia datelor personale;
- personalul extern care asigură mentenanţa infrastructurii IT din cadrul firmei;
- angajaţilor **SOLAR POWER MANGEMENT SRL** .

TERMENI ŞI DEFINIŢII:

ANSPDCP = Autoritatea Naţională 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 şi de identificare în anumite sisteme informatice de către persoanele autorizate;

Date cu caracter personal = orice informaţii 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 mulţi factori specifici identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

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

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

Operator - Persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevazute 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 autorităţile publice, instituţiile şi structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului;

Responsabilul cu protecţia datelor – persoana desemnată cu:

- Informarea şi consilierea operatorului precum şi a angajaţilor cu privire la obligaţiile care le revin referitoare la protecţia datelor;
- Monitorizarea respectării regulamentului GDPR şi a politicilor operatorului în ceea ce priveşte protecţia datelor cu caracter personal, inclusiv acţiunile de sensibilizare şi de formare a personalului;
- Furnizarea de consiliere în ceea ce priveşte evaluarea impactului asupra protecţiei datelor şi monitorizarea funcţionării acesteia;
- Cooperarea cu autoritatea de supraveghere;
- Asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare.

Prelucrarea datelor cu caracter personal - orice operaţiune sau set de operaţiuni 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 terţi prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;
Stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, respectand în acelasi timp protecţia datelor cu caracter personal „începând cu momentul conceperii şi în mod implicit" (by design and by default);
Utilizator - 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.

1. CONDIŢII DE LEGITIMITATE

SOLAR POWER MANGEMENT SRL prelucrează datele cu caracter personal înregistrate în sistemele IT ale firmei, respectând prevederile legale în domeniu.

1.1 Referinţe normative:

a) Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare;
b) Ordinul nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal;
c) Decizia nr. 200 din 14 decembrie 2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea, precum şi pentru modificarea şi abrogarea unor decizii;
d) Ordinul Avocatului Poporului nr. 52 din 18/04/2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal;
e) Decizia ANSPDCP nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video;
f) Decizia ANSPDCP nr. 132 din 20/12/2011 privind condiţiile prelucrării codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală;
g) 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 Transparenţă

Procedură de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal este disponibilă ca anexă a Regulamentului de Ordine Interioară **SOLAR POWER MANGEMENT SRL .**

1.3 Revizuiri periodice

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

- îndeplinirea scopului declarant;
- posibile îmbunătăţiri ale **Procedurii de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal.**

2. Reguli Generale

Prin cerinţe minime de securitate aplicate în cadrul **SOLAR POWER MANGEMENT SRL ,** 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 si luand in considerare cerintele din legislatia nationala, deciziile ANSPDCP în acest domeniu şi Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date.

SOLAR POWER MANGEMENT SRL 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 **SOLAR POWER MANGEMENT SRL** , persoane responsabile cu respectarea dispoziţiilor Legii nr.677/2001.

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

Activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, este în responsabilitatea Responsabilului cu

Protecția Datelor cu Caracter Personal / Data Protection Officer, care este anunțat despre incidentul privind datele cu caracter personal în cel mai scurt timp.

Activitățile pe care le efectuează DPO sunt:

- ✓ Se documentează despre datele deținute în cazul repectiv;
- ✓ Se asigură că petentul are calitatea legală pentru a cere respectarea dreptului prevăzut de GDPR;
- ✓ Documentează baza legală a prelucrărilor de date implicate;
- ✓ Dispune măsurile necesare pentru elaborarea răspunsului / rezolvarea petiției respective, respective a incidentului semnalat privind datele cu carcater personal dacă acestea implică și alte operațiuni decât informarea;
- ✓ Elaborează răspunsul către petent;
- ✓ Asigură dialogul cu ANSPDCP și elaborează răspunsul / răspunsurile către ANSPDCP, respectând prevederile Regulamentul (UE) 2016/679 și ale legislației în vigoare;
- ✓ Aplică prevederile referitoare la activitatea de dialog cu petentul și cu ANSPDCP, împreună cu alte măsuri și prevederi aprobate în cadrul **SOLAR POWER MANGEMENT SRL** prin sistemul de proceduri de implementare a GDPR anexe la Regulamentul de Ordine Interioară **SOLAR POWER MANGEMENT SRL** ;
- ✓ Se asigură de respectarea deciziilor, respectiv de aplicarea măsurilor legale prevăzute de GDPR.

3. Activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

3.1. Timpul de raspuns la un incident semnalat / petiție / solicitare venită din partea persoanelor interesate, respectiv a persoanele fizice vizate de prelucrarea datelor cu caracter personal, conform legislației europene prin aplicarea Regulamentului nr. 679/2016

În conformitate cu Articolului 12, Alineatul 3 din Regulamentul nr. 679/2016: timpul maxim de răspuns la o petiție / solicitare / incident semnalat este de 30 de zile.

SOLAR POWER MANGEMENT SRL , ca operator, se obligă să furnizeze persoanei vizate informații privind acțiunile întreprinse în urma unei cereri fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii.

Atunci când e necesar, din motive legate de complexitatea şi volumul cererilor primite simultan, această perioadă poate fi prelungită până la două luni. Chiar şi în aceste condiţii de prelungire, **SOLAR POWER MANGEMENT SRL** va informa persoana vizată de această prelungire tot în intervalul de o lună. Pentru cererile trimise în format electronic, informaţiile vor fi furnizate în format electronic – acolo unde este posibil, cu excepţia cazului în care persoana vizată solicită informațiile într-un alt format.

3.2. Persoanele indreptățite să depună o plâgere referitoare la prelucrarea datelor cu caracter personal în cadrul SOLAR POWER MANGEMENT SRL

Plângerile, sesizările şi cererile pot fi depuse personal sau prin reprezentant, de către persoanele îndreptățite să depună o plângere referitoare la prelucrarea datelor cu caracter personal, cu menţionarea obligatorie a numelui, prenumelui, adresei de domiciliu sau de corespondenţă şi a semnăturii persoanei fizice.

În cazul în care plângerile, sesizările şi cererile se depun prin reprezentant, sunt obligatorii datele de identificare ale acestuia (nume, prenume, adresă de domiciliu sau de corespondenţă/denumire, sediu şi adresă de corespondenţă) şi anexarea împuternicirii semnate de persoana interesată.

În cazul plângerilor, sesizărilor şi cererilor transmise prin poştă electronică sau on-line, este obligatorie menţionarea unei adrese valabile de poştă electronică pentru contactarea petiţionarului.

Toate plângerile, sesizările şi cererile depuse în cadrul **SOLAR POWER MANGEMENT SRL** de catre persoanele fizice interesate, vor fi înregistrate obligatoriu cu număr de înregistrare în registrul de intrare – ieşire a documentelor în cadrul **SOLAR POWER MANGEMENT SRL** .

Plângerile, sesizările şi cererile în care nu se precizează datele de identificare ale petiţionarului, respectiv, nume, prenume, adresă de domiciliu sau corespondenţă, sunt considerate anonime. Acestea nu se înregistrează, se clasează cu această menţiune în registrul de intrare – ieşire a documentelor in cadrul **SOLAR POWER MANGEMENT SRL .**

În cazul în care un petiţionar adresează mai multe petiţii / sesizari, sesizând aceeaşi problemă, respectiv acelaşi incident, acestea se conexează, petiţionarul urmând să primească un singur răspuns care trebuie să facă referire la toate petițiile / sesizările depuse de către petiționar.

3.3. Drepturile persoanelor fizice vizate de prelucrarea datelor cu caracter personal

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice (denumit și GDPR) vine cu unele drepturi noi pentru indivizi și consolidează unele dintre drepturile care existau deja în Legislația Europeană.

Astfel, GDPR oferă persoanelor fizice vizate de prelucrarea datelor cu caracter personal următoarele drepturi generale:

- ✓ dreptul de a fi informat;
- ✓ dreptul de acces;
- ✓ dreptul la rectificare;
- ✓ dreptul de ștergere;
- ✓ dreptul de a restricționa procesarea;
- ✓ dreptul la portabilitatea datelor;
- ✓ dreptul la obiect (sau dreptul de a ridica obiecții);
- ✓ drepturi legate de luarea de decizii automatizate și de profilare.

4. Prelucrarea și protecția datelor

Prelucrarea datelor cu caracter personal în cadrul **SOLAR POWER MANGEMENT SRL** se realizează cu respectarea cerințelor legale și în condiții care să asigure securitatea, confidențialitatea și respectarea drepturilor generale ale persoanelor vizate prezentate mai sus, amănunțit în această procedură, respectiv: dreptul de a fi informat , dreptul de acces, dreptul la rectificare, dreptul de ștergere, dreptul de a restricționa procesarea, dreptul la portabilitatea datelor, dreptul la obiect (sau dreptul de a ridica obiecții), drepturi legate de luarea de decizii automatizate și de profilare.

Procedura specifică de acces, prelucrare și protecție a datelor este disponibilă ca anexă a Regulamentului de Ordine Interioară **SOLAR POWER MANGEMENT SRL .**

5. 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, vor respecta **Procedura specifică de acces, prelucrare și protecție a datelor cu caracter personal**.

5.1. Exercitarea drepturilor de acces, intervenţie şi opoziţie

Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc, de a solicita intervenţia (ştergere/actualizare/rectificare/anonimizare) sau de a se opune prelucărilor, conform legii. Orice cerere de a accesa, rectifica, bloca şi/sau şterge date cu caracter personal ar trebui să fie adresată **SOLAR POWER MANGEMENT SRL** , iar o copie a acesteia trebuie trimisă către Responsabilul cu Protecţia Datelor Personale.

Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune şi în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane.

6. Activitatea de răspuns la incidentele privind datele cu caracter personal, în legătură cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal

Conform **Articolului 33** din GDPR va fi obligatoriu ca o organizaţie cu rol de operator să raporteze autorităţii sale de supraveghere orice breşă de securitate a datelor personale în termen de 72 de ore de la conştientizarea acesteia. Dacă această cerinţă nu este îndeplinită, raportul final trebuie însoţit de o explicaţie a întârzierii. Notificarea trebuie să includă informaţii specifice, inclusiv o descriere a măsurilor luate pentru a soluţiona breşa şi pentru a atenua posibilele efecte secundare.

În cazul în care breşa poate avea ca rezultat un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, indivizii înşişi trebuie să fie contactaţi „fără întârzieri nejustificate". Acest contact nu va fi necesar dacă există măsuri de protecţie adecvate – în esenţă, criptare – pentru a elimina pericolul pentru persoanele vizate.

În **Articolul 33 – Notificarea unei încălcări a datelor cu caracter personal către autoritatea de supraveghere**, se specifică foarte clar că:

- Raportarea în situaţia apariţiei unor breşe de securitate este obligatorie pentru orice operator de date personale;
- Operatorii trebuie să raporteze către autorităţilor de supraveghere competente orice încălcare a condiţiilor de siguranţă fără întârzieri nejustificate;
- Dacă este posibil, nu mai târziu de 72 de ore de la prima conştientizare;
- Dacă raportarea nu este făcută în termen de 72 de ore, trebuie furnizată o justificare a întârzierii;

- Nu este necesară notificarea cazurilor în care încălcarea este «puțin probabil să ducă la un risc pentru drepturile și libertățile» persoanelor vizate;
- Dacă breșa de securitate este constatată de către un procesator de date, acesta trebuie să notifice operatorul cu care colaborează fără întârzieri nejustificate.

6.1. Informații incluse în notificarea unei breșe de securitate

Elementele esențiale care trebuie să se regăsească într-o notificare se referă la:

- natura încălcării datelor cu caracter personal;
- categoriile și numărul aproximativ al persoanelor implicate;
- categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- numele și datele de contact ale responsabilului cu protecția datelor (în cazul în care organizația dvs. dispune de unul) sau orice alt punct de contact de unde pot fi obținute mai multe informații;
- descriere a consecințelor probabile ale încălcării datelor cu caracter personal;
- descriere a măsurilor luate sau propuse a fi luate pentru a face față încălcării datelor cu caracter personal dacă este cazul, o descriere a măsurilor luate pentru a atenua eventualele efecte adverse.

6.2. Situații în care nu se notifică persoanele vizate

În **Articolul 34: Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal, Alineatul 3,** regulamentul stipulează că informarea persoanei vizate nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiții:

✓ operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar acestea au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

✓ operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se materializeze;

✓ informarea ar necesita un efort disproporționat. În această situație, se efectuează în loc, o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

6.3 Ghidul recomandărilor legate de anunțarea breșelor de Securitate

De pe site-ul oficial al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) poate fi descărcat **"Ghidul privind notificarea încălcărilor de securitate"**, un instrument deosebit de util în implementarea condițiilor impuse de GDPR, elaborate de Grupul de Lucru, Articolul 29.

Tot de pe site-ul Autorității Naționale pot fi accesate și consultate formularele utilizate deja în notificarea breşelor de securitate conform legislației actuale.

Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.