

Politică Generală privind protecția datelor cu caracter personal

A

ASOCIATIEI ROMANE PENTRU ENERGIE EOLIANA - RWEA

1. Prezentare generală

1.1. Introducere

Asociația Română pentru Energie Eoliană - Rwea, prelucrează date cu caracter personal referitoare la persoane fizice. Acestea pot reprezenta date în legătură cu clienții, furnizorii, contacte pentru afaceri, angajați și alte persoane cu care asociația/organizația a încheiat un contract sau cu care aceasta se află într-o legătură de reprezentare.

Această politică descrie modul în care datele personale trebuie colectate, utilizate și stocate pentru a fi în concordanță cu standardele GDPR referitoare la protecția datelor – și, de asemenea, să îndeplinească condiția legalității.

Acest control se aplică tuturor sistemelor, persoanelor și proceselor care constituie sistemele informatice ale asociației, inclusiv directorii, angajații, furnizorii și alte părți terțe care au acces la sistemele societății.

1.2. Existența politicii

Această politică privitoare la protecția datelor asigură Asociația referitor la conformitatea cu legislația privind protecția datelor cu caracter personal și practicile performante la acest nivel și anume:

- Protecția drepturilor persoanelor vizate (de exemplu: a clienților persoane fizice, angajaților și a partenerilor cu care asociația colaborează);
- Modul de stocare și prelucrare a datelor persoanelor fizice și angajaților asociației;
- Protecția companiei de posibilele riscuri referitoare la încălcarea securității datelor.

1.2.1 Legislația privitoare la protecția datelor cu caracter personal

Regulamentul (EU) nr. 679/2016 descrie modul în care organizația – incluzând și Asociația Română pentru Energie Eoliană - Rwea, trebuie să colecteze și să prelucreze datele cu caracter personal. Amenzile semnificative sunt aplicabile în cazul în care se consideră că o încălcare a

fost sesizata în temeiul Regulamentului GDPR, si care are rolul de a proteja datele cu caracter personal ale cetățenilor Uniunii Europene.

Aceste reguli se aplică indiferent dacă datele sunt stocate în format electronic, pe hârtie sau pe alte materiale.

Pentru a fi în concordanță cu legislația, informațiile personale trebuie să fie colectate și utilizate în mod corect, stocate în siguranță, nepermițându-se folosirea acestora în mod ilegal.

Regulamentul (EU) nr 2016/679 stipulează, printre altele, faptul că datele personale trebuie:

1. Să fie prelucrate în mod legal, echitabil și transparent față de persoana vizată („*legalitate, echitate și transparență*”);
2. Să fie c olectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri („*limitări legate de scop*”);
3. Să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („*reducerea la minimum a datelor*”);
4. Să fie exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („*exactitate*”);
5. Să **nu** fie păstrate mai mult timp decât este necesar („*limitări legate de stocare*”);
6. Să fie prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („*integritate și confidențialitate*”);
7. Să fie prelucrate în concordanță cu drepturile persoanelor vizate;
8. Să **nu** fie transferate în afara Spațiului Economic European, decât în cazul în care teritoriul/țara unde urmează a fi transferate asigură un nivel adecvat de protecție a datelor cu caracter personal.

1.2.2 Definiții

Există un număr total de 26 de definiții enumerate în cadrul GDPR și nu este adecvată reproducerea acestora aici. Cu toate acestea, definițiile cele mai fundamentale cu privire la această politică sunt următoarele:

| | |
|---|--|
| <i>Date cu caracter personal</i> | orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”) |
| <i>Persoana vizată</i> | o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau |

| | |
|---|--|
| | indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale |
| <i>Prelucrare</i> | orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea |
| <i>Operator</i> | persoana fizică sau juridică, autoritatea publică, agenția sau alt 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 |
| <i>Persoană împuternicită de operator</i> | persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului |

1.3. Principii privind prelucrarea datelor cu caracter personal

Există o serie de principii fundamentale pe care se bazează prelucrarea datelor personale conform Regulamentului GDPR.

Datele personale sunt:

- (a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („**legalitate, echitate și transparență**”);
- (b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în

interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) („**limitări legate de scop**”);

- (c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („**reducerea la minimum a datelor**”);
- (d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („**exactitate**”);
- (e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („**limitări legate de stocare**”);
- (f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („**integritate și confidențialitate**”).

Asociația, se va asigura că respectă toate aceste principii atât în procesul de prelucrare pe care îl desfășoară în prezent, cât și ca parte a introducerii de noi metode de procesare, cum ar fi noile sisteme informatice.

1.4. Drepturile persoanei vizate

Persoana vizată are, de asemenea, drepturi în temeiul Regulamentului GDPR. Acestea constau în:

- Dreptul de retragere a consimțământului;
- Dreptul la informare;
- Dreptul de acces;
- Dreptul la rectificare;
- Dreptul la ștergerea datelor („dreptul de a fi uitat”);
- Dreptul la restricționarea prelucrării;
- Dreptul la portabilitatea datelor;
- Dreptul de a se opune prelucrării;

- Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri;
- Dreptul de a depune o plângere la Autoritatea de Supraveghere;
- Dreptul de a se adresa justiției.

Fiecare dintre aceste drepturi este susținută de proceduri adecvate din partea Asociației, care permit ca acțiunea necesară să fie luată în termenele stabilite de Regulamentul GDPR.

Persoanele vizate își pot exercita o parte din drepturile de mai sus prin e-mail, adresate operatorului. Operatorul de date poate atașa o cerere standard, cu toate că persoanele nu sunt obligate să o folosească.

Cererile vor fi scutite de vreo taxă. Operatorul va fi obligat să furnizeze răspuns în maxim o lună, iar în anumite cazuri excepționale în cel mult două luni de la primirea cererii.

Operatorul de date va verifica întotdeauna identitatea oricărei persoane. În vederea răspunderii la cereri și permiterea exercitării drepturilor, departamentul juridic sau consultanții juridici externi vor avea un cuvânt de spus cu privire la temeinicia cererii.

Asociația, respectă următoarele termene pentru răspunsul la cererile persoanelor vizate:

| Solicitarea de date solicitate | Grafic de timp |
|--|---|
| <i>Dreptul de a fi informat</i> | Atunci când se colectează date (dacă acestea sunt furnizate de persoana vizată) sau în termen de o lună (dacă nu sunt furnizate de persoana vizată) |
| <i>Dreptul de acces</i> | O lună |
| <i>Dreptul la rectificare</i> | O lună |
| <i>Dreptul de ștergere</i> | Fără întârzieri nejustificate |
| <i>Dreptul de a restricționa procesarea</i> | Fără întârzieri nejustificate |
| <i>Dreptul la portabilitatea datelor</i> | O lună |
| <i>Dreptul de a se opune prelucrării</i> | La primirea obiecției |
| <i>Drepturi legate de procesul de luare a deciziilor și profilaxie automată.</i> | Nespecificat |

1.5. Temeiurile prelucrării

Există șase moduri alternative în care poate fi stabilită legalitatea unui caz specific de prelucrare a datelor cu caracter personal în cadrul Regulamentului GDPR.

1.5.1 Consimțământul

Cu excepția cazului în care este necesar dintr-un motiv admis în Regulamentul GDPR, Asociația, va obține întotdeauna acordul explicit din partea unei persoane vizate pentru colectarea și prelucrarea datelor. În cazul copiilor sub vârsta de 16 ani (o vârstă mai mică poate fi permisă în anumite state membre ale UE), va fi obținut consimțământul părinților. Informații transmise despre utilizarea datelor noastre cu caracter personal vor fi furnizate persoanelor vizate în momentul obținerii consimțământului și explicării drepturilor acestora cu privire la datele lor, cum ar fi dreptul de retragere a consimțământului. Aceste informații vor fi furnizate într-o formă accesibilă, scrisa în limbaj clar și gratuit.

În cazul în care datele cu caracter personal nu sunt obținute direct de la persoana vizată, aceste informații vor fi furnizate persoanei vizate într-o perioadă rezonabilă de timp după obținerea datelor.

1.6. Încheierea sau executarea unui contract

În cazul în care datele cu caracter personal colectate și prelucrate sunt necesare pentru a încheia sau executa un contract cu persoana vizată, nu este necesar consimțământul explicit. Acesta va fi cazul în care contractul nu poate fi încheiat fără datele personale în cauză, *de exemplu* o livrare nu poate fi efectuată fără o adresă la care să se poată livra.

1.7. Obligația legală

În cazul în care datele cu caracter personal trebuie să fie colectate și prelucrate pentru a ne conforma legii, nu este necesar consimțământul explicit. Acest lucru poate fi în cazul anumitor date referitoare la ocuparea forței de muncă și la impozitare, de exemplu.

1.8. Interesele vitale ale subiectului datelor

În cazul în care datele cu caracter personal sunt necesare pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice, atunci acesta poate fi utilizat ca temeiul legal al prelucrării. Asociația, va păstra dovezi rezonabile, documentate că acest lucru sa poata fi verificat daca este cazul, ori de câte ori acest motiv este utilizat ca bază legală pentru prelucrarea datelor cu caracter personal.

1.9. Activitatea desfășurată în interes public

În cazul în care Asociația, trebuie să îndeplinească o sarcină pe care o consideră a fi în interesul public sau ca parte a unei obligații oficiale, atunci nu va fi solicitat consimțământul persoanei vizate. Evaluarea interesului public va fi documentată și pusă la dispoziție ca dovezi atunci când este necesar.

1.10. Interesul legitim

Dacă prelucrarea datelor cu caracter personal este necesară în interesul legitim al Societății și este considerată că nu afectează în mod semnificativ drepturile și libertățile persoanei vizate, atunci aceasta poate fi definită ca fiind motivul legal al prelucrării. Din nou, raționamentul din spatele acestui punct de vedere va fi documentat.

2. Persoane fizice, riscuri și responsabilități

2.1. Domeniul politicii

Prezenta politică se aplică:

- Sediilor și punctelor de lucru ale asociației;
- Tuturor departamentelor din cadrul asociației;
- Întregului personal al asociației;
- Tuturor contractanților, furnizorilor și altor persoane ce lucrează în numele asociației.

Are aplicabilitate asupra tuturor datelor pe care Asociația le deține în legătură cu persoanele fizice identificabile. Acestea pot cuprinde:

- Numele și prenumele persoanelor fizice;
- Adresele poștale;
- Adresele de e-mail;
- Numerele de telefon;
- Conturi bancare;
- Semnatura.

și orice alte date referitoare la o persoană fizică identificată sau identificabilă.

2.2. Riscurile

Politica ajută la protejarea Asociației, la reale riscuri, la nivel de securitate, incluzând:

- Încălcări ale confidențialității.
- Vătămarea reputației.

2.3. Responsabilități

Oricine lucrează pentru sau cu Asociația Română pentru Energie Eoliană - Rwea, își angajează răspunderea pentru a asigura colectarea, prelucrarea, stocarea și utilizarea datelor cu caracter personal în mod corespunzător.

Fiecare echipă care utilizează datele personale trebuie să asigure faptul că acestea sunt utilizate și prelucrate în concordanță cu politica și principiile generale ale protecției datelor.

Aceste persoane au următoarele **atribuții**:

- ❖ Conducerea este responsabilă cu privire la asigurarea îndeplinirii în mod legal a obligațiilor de către Asociație;
- ❖ Managerul IT este responsabil pentru:
 - Asigurarea tuturor sistemelor, serviciilor și echipamentului folosit pentru a stoca datele, în condițiile unor standarde adecvate de Securitate, asigurând confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
 - Efectuarea verificărilor și scanărilor în mod constant pentru a asigura nivelul înalt de securitate al hardware-ului și software-ului, precum și funcționarea decentă a lor;
 - Evaluarea fiecărui serviciu al terțului pe care compania îl consideră că utilizează sau stochează date. *De exemplu:* servicii de cloudcomputing.
 - Implementează măsuri pentru pseudonimizarea și criptarea datelor cu caracter personal;
 - Implementează măsuri pentru a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

3. Regulamentul general al personalului

- ➔ Singurele persoane care sunt apte să acceseze datele prezentate în această politică ar trebui să fie doar cele care folosesc datele cu caracter personal în activitatea pe care o realizează.
- ➔ Datele ar trebui să nu fie împărtășite către toți angajații. Când este necesar accesul la informații confidențiale se poate face doar cu aprobare de la conducerea Societății.

- ➔ Asociația, prin conducerea sa va asigura trainingul aferent tuturor angajaților pentru a-i ajuta în procesul înțelegerii responsabilității pe care o au în momentul în care utilizează datele.
- ➔ Angajații ar trebui să asigure securitatea datelor luând măsuri și folosind instrucțiunile de mai jos:
- ➔ Vor trebui utilizate parole puternice;
- ➔ Datele personale nu vor fi dezvăluite către persoane neautorizate, fie din interiorul companiei / organizației sau în afară;
- ➔ Datele ar trebui să fie revizuite și actualizate dacă există situația în care datele nu sunt concordante cu realitatea. Dacă nu mai sunt necesare, datele vor fi anonimizate sau vor fi șterse.
- ➔ Angajații vor cere ajutorul managerului lor sau responsabilului cu protecția datelor dacă nu sunt siguri în legătura cu orice aspect al protecției datelor.

4. Stocarea datelor

Aceste reguli descriu cum și unde ar trebui să fie stocate datele cu caracter personal. Întrebările despre stocarea datelor pot fi redirecționate în siguranță managerului IT sau Operatorului de date.

Când datele sunt **stocate** pe **hârtie**, ele trebuie păstrate într-un loc sigur unde persoanele neautorizate nu pot avea acces.

Aceste instrucțiuni se aplică, de asemenea, asupra datelor care sunt stocate în mod obișnuit în format electronic, dar au fost printate din anumite considerente:

- Hârtiile sau fișierele ar trebui păstrate într-un loc închis sau într-un sertar închis;
- Angajații ar trebui să se asigure că hârtia sau cele printate nu sunt lăsate către oameni neautorizați ce ar putea să le vadă, ca de exemplu pe imprimantă;
- Printurile ar trebui distruse când nu mai sunt necesare.

Când datele sunt **stocate** în **format electronic**, ele trebuie să fie protejate de accesul neautorizat, ștergerilor accidentale sau atacurilor intenționate de hacking:

- Datele ar trebui protejate de parole puternice ce sunt schimbate regulat și niciodată împărtășite între angajați;
- Dacă datele sunt stocate pe suporturi amovibile (precum CD, DVD), acestea ar trebui păstrate în siguranță atunci când nu sunt folosite;
- Datele ar trebui stocate numai în servere sau unități specializate și ar trebui să fie încărcate într-un serviciu de cloudcomputing aprobat;

- Serverele ce conțin informații personale ar trebui plasate într-un loc sigur, departe de spațiul general de birouri;
- Datele nu ar trebui salvate direct pe laptopuri sau alte dispozitive mobile precum tablete sau smartphone-uri.
- Datele ar trebui să aibă un back-up. Aceste backup-uri ar trebui testate regulat.
- Toate serverele și calculatoarele ce conțin date ar trebui protejate de software de Securitate și firewall.

5. Utilizarea datelor

Datele personale nu au nicio valoare pentru Asociație, decât dacă aceasta le poate folosi în activitatea sa. Se întâmplă atunci când datele sunt accesate și folosite, iar acest fapt poate fi predispus la numeroase riscuri, corupție sau chiar furt:

- Când se lucrează cu date personale, angajații ar trebui să asigure ecranele calculatoarelor, sunt întotdeauna închise când le lasă nesupravegheate;
- Datele personale nu ar trebui transmise prin e-mail, având în vedere că aceasta cale de comunicare nu este sigură.
- Datele ar trebui criptate înainte de a fi transferate electronic. Managerul IT ar trebui să explice cum sunt trimise datele către contactele externe autorizate.
- Datele personale nu ar trebui transferate în afara Spațiului Economic European.
- Angajații ar trebui să nu salveze datele personale în dispozitivele lor personale. Întotdeauna ar trebui să existe acces și actualizare a copiei centrale a tuturor datelor.

6. Precizia datelor

Legislația solicită Asociației, să urmărească pașii în mod rezonabil pentru a asigura precizia și actualizarea datelor.

Acuratețea datelor este foarte importantă și este necesar un efort considerabil din partea Societății, pentru a o asigura.

Este responsabilitatea tuturor angajaților care lucrează cu aceste date să urmărească pașii pentru a asigura acuratețea și actualitatea datelor pe cât posibil.

- Datele vor fi păstrate în puține locuri. Personalul nu trebuie să creeze alte locuri adiționale deloc necesare, ca de exemplu: copii inutile;
- Personalul ar trebui să se folosească de fiecare oportunitate pentru a asigura actualizarea datelor. *De exemplu:* prin confirmarea unor detalii în momentul în care clientul sună;
- Asociația Română pentru Energie Eoliană - Rwea, va depune toate diligențele necesare pentru ca subiectul datelor să își poată actualiza informațiile pe care societatea le deține.

- Datele ar trebui actualizate când se descoperă inadvertențe. De exemplu: când un membru/client nu mai poate fi contactat prin intermediul unui număr de telefon, se recomandă eliminarea din baza de date a Asociației a acestui număr.

7. Divulgarea datelor din alte motive

În anumite circumstanțe, legislația permite datelor personale să fie dezvăluite către organele legii fără consimțământul persoanei subiect al datelor.

În aceste circumstanțe, Asociația, va dezvălui datele necesare. Operatorul de date va asigura faptul că cererea este legitimă, căutând asistență de la responsabilul cu protecția datelor al organizației (atunci când este necesar).

8. Furnizare informații către persoanele vizate

Asociația noastră țintește spre a asigura faptul că persoanele vizate știu cum sunt prelucrate datele, asigurându-se că ei înțeleg:

- Cum sunt datele lor utilizate;
- Cum își pot exercita drepturile.

9. Consecințe

Nerespectarea prezentei Politici de către angajații Asociației sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse organizației, ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), Asociația va denunța activitatea infracțională organelor în drept, pentru respectarea legii și pentru tragerea la răspundere penală a făptuitorului.

Prezenta Politică va fi adusă de către conducerea Asociației la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.