POLITICA DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

ÎN CADRUL MAZARINE ENERGY ROMANIA S.R.L.

Operator:

MAZARINE ENERGY ROMANIA S.R.L.

Șos. București – Ploiești 42-44

Băneasa Business & Technology Park, corp B, aripa B2, et. 1, cam. 1

Sector 1, București

Telefon: 0371.151.172, Fax: 0372.891.488, Email : gdpr.romania@mazarine.energy

Date de contact ale responsabilului cu protecția datelor:

Șos. București – Ploiești 42-44

Băneasa Business & Technology Park, corp B, aripa B2, et. 1, cam. 1

Sector 1, București

Telefon: 0748.146.100, Email: dpo.romania@mazarine.energy

Intocmită de	**Aprobată de**
Ciută Oana Sabina	**Spencer Florian Coca**
Responsabil cu Protecția Datelor	**Reprezentant Permanent al Administratorului**
Prezenta politică a fost revizuită și aprobată la data de 15.07.2023	

Preambul

Considerăm asigurarea dreptului la protecția datelor cu caracter personal ca un angajament fundamental al MAZARINE ENERGY ROMANIA S.R.L., prin urmare vom dedica toate resursele și eforturile necesare pentru a prelucra datele personale în deplină concordanță cu Regulamentul (UE) 2016/679 "Regulamentul General privind Protecția Datelor" sau "GDPR"), precum și cu orice altă legislație aplicabilă pe teritoriul României. Întrucât unul dintre principiile esențiale ale acestui cadru este ***transparența,*** am întocmit politica internă de protecție a datelor cu caracter personal, în care detaliem modul în care colectăm, utilizăm, transferăm și protejăm datele cu caracter personal aparținând angajaților, clienților, colaboratorilor și a altor persoane atunci când este cazul.

Ne rezervăm dreptul de a actualiza și modifica periodic această Politică în concordanță cu modificările impuse de legislația în domeniu.

Capitolul 1

Documente de referință

1. Regulamentul (UE) 679 / 2016, al Parlamentului European si al Consiliului, privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date;
2. Legea nr. 190 / 2018, privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date;
3. Web: site-ul Comisiei Europene: https://ec.europa.eu/;
4. Web: site-ul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal: dataprotection.ro.

Capitolul 2

Scopul politicii de protecție a datelor

Prezentul document, are drept scop principal, stabilirea politicii MAZARINE ENERGY ROMANIA S.R.L., atât cu privire la protecția datelor cu caracter personal pe care Societatea le prelucrează în cadrul activităților sale, în relațiile cu salariații, clienții săi sau alte persoane vizate, cât și garantarea și protejarea drepturilor și libertăților

fundamentale ale persoanelor vizate, în special a dreptului la viața intimă, familială și privată, în contextul prelucrării datelor cu caracter personal.

Ca parte a responsabilității sale sociale, MAZARINE ENERGY ROMANIA S.R.L., se angajează să respecte legile naționale și internaționale privind protecția datelor. În consecință, prezenta politică se bazează pe principii acceptate la nivel european și global, în ceea ce privește protecția datelor. Această politică de protecție a datelor, se aplică în întreaga Societate, urmând a fi respectată întocmai, de către salariații și/sau colaboratorii/partenerii de afaceri ai Societății, ori de câte ori aceștia prelucrează date cu caracter personal în cursul și pe durata exercitării îndatoririlor lor profesionale.

Asigurarea protecției datelor, reprezintă fundamentul relațiilor în afaceri de încredere și reputația Societății noastre. MAZARINE ENERGY ROMANIA S.R.L., în cadrul activităților desfașurate, prelucrează date cu caracter personal pentru executarea contractelor (individuale, comerciale etc), în vederea îndeplinirii unor obligații legale, în scopul intereselor sale legitime, în scop de marketing etc.

Politica de protecție a datelor, prevede condițiile – cadru necesare asigurării nivelului adecvat de protecție a datelor, prevăzute de Regulamentul (UE) nr. 679 / 2016, oferind o prezentare generală a cerințelor minime privind protecția persoanelor fizice, în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Capitolul 3

Termeni și definiții

1. **„date cu caracter personal”,** înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoană vizată”); 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;
2. **”date cu caracter special”**, sunt datele despre originea rasială sau etnică, despre opiniile politice, confesiunea religioasă sau convingerile filozofice, apartenența la sindicate sau calitatea de membru al unor organizații, prelucrarea de date genetice, de date biometrice, date privind cazierul judiciar sau sănătatea, date privind viața sexuală sau orientarea sexuală a unei personane fizice;
3. **„GDPR”, „RGPD”** sau **„Regulamentul”** înseamnă REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
4. **”persoana vizată”**, în cadrul acestei politici de protecție a datelor, este orice persoană fizică, ale cărei date cu caracter personal pot fi prelucrate;

5. **„prelucrare"** înseamnă 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;
6. **„restrictionarea prelucrarii"** înseamnă marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea viitoare a acestora;
7. **„creare de profiluri"** înseamnă orice formă de prelucrare automată a datelor cu caracter personal, care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, ăn special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respective sau deplasările acesteia;
8. **„pseudonimizare"** înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod, încât acestea să nu mai poata fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
9. **„sistem de evidență a datelor"** înseamnă orice set structurat de date cu caracter personal accesibile, conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
10. **„operator"** înseamnă 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;
11. **„persoana împuternicită de operator"** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism, care prelucreaza datele cu caracter personal in numele operatorului;
12. **„destinatar"** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism, căreia / căruia îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern, nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective, respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;
13. **„parte terță"** înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism, altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
14. **"țările terțe"**, în cadrul politicii de protecție a datelor cu caracter personal, sunt toate națiunile din afara Uniunii Europene / SEE. Aceasta nu include țările cu un nivel de protecție a datelor considerat suficient de către Comisia Europeană;
15. **"Spațiul Economic European"** (SEE), este o regiune economică asociată cu UE, și include: Norvegia, Islanda și Liechtenstein;
16. **„consimțământ"** al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate, prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
17. **„încălcarea securității datelor cu caracter personal"** înseamnă o încalcare a securității, care duce, în mod accidental sau ilegal la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor

cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

18. **„date genetice"** înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care ofera informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;
19. **„date biometrice"** înseamnă datele cu caracter personal care rezultă în urma unor tehnici de prelucrare specific, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi, imaginile faciale sau datele dactiloscopice;
20. **„date privind sanatatea"** înseamnă datele cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;
21. **„reprezentant"** înseamnă o persoană fizică sau juridică, stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, în temeiul articolului 27, care reprezintă operatorul sau persoana împuternicită, în ceea ce privește obligațiile lor respective, care le revin în temeiul prezentului Regulament;
22. **„întreprindere"** înseamnă o persoană fizică sau juridică, ce desfășoara o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații, care desfașoara în mod regulat o activitate economică;
23. **„autoritate de supraveghere"** înseamnă o autoritate publică independentă, instituită de un stat membru, în temeiul articolului 51;
24. **„obiecție relevantă și motivată"** înseamnă o obiecție la un proiect de decizie, în scopul de a stabili dacă există o încălcare a prezentului Regulament sau dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul Regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile, libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii;
25. **„utilizatori"** înseamnă 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.

Capitolul 4

Domeniul de aplicare și modificarea politicii

Această politică de protecție a datelor cu caracter personal, se aplică tuturor angajaților MAZARINE ENERGY ROMANIA S.R.L. și se aplică în întreaga Sociatate, urmând a fi respectată întocmai, ori de câte ori se prelucrează date cu caracter personal în cursul și pe durata exercitării îndatoririlor profesionale.

Politica privind protecția datelor, se extinde peste toate prelucrările de date cu caracter personal efectuate de către MAZARINE ENERGY ROMANIA S.R.L. în cadrul activităților sale, în relațiile cu salariații, clienții săi sau alte persoane vizate.

Datele anonimizate (respectiv, acele informații care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoana identificată sau identificabilă), acolo unde există, utilizate de exemplu pentru evaluări statistice sau alte studii, nu sunt supuse acestei politici de protecție a datelor.

Politica de protecție a datelor cu caracter personal este revizuită anual, dacă este necesar, iar cea mai recentă versiune, aprobată de Reprezentantul Permanent al Administratorului, va fi imediat disponibilă, atât angajaților MAZARINE ENERGY ROMANIA S.R.L., cât și partenerilor/consultanților/terților, pe site-ul web: www.cfrcalatori.ro.

Capitolul 5

Principii pentru prelucrarea datelor cu caracter personal

Art. 1. Corectitudinea și legalitatea

La prelucrarea datelor cu caracter personal, drepturile individuale ale persoanelor vizate trebuie protejate. Datele personale trebuie colectate și prelucrate în mod legal și corect. **Prelucrarea este legală, numai dacă și în măsura în care, se aplică cel puțin una dintre următoarele condiții:**

- persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
- prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
- prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Art. 2. Restricție la un anumit scop

Datele cu caracter personal pot fi prelucrate, numai în scopul definit **înainte de colectarea datelor si comunicat persoanei vizate.** Modificările ulterioare ale scopului, sunt posibile doar într-o măsură limitată și necesită o fundamentare solidă. Conform art. 13 alin. (3) din Regulamentul (UE) 679 / 2016, în cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea

au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante.

Art. 3. Transparenţă

Principiul transparenţei prevede că, orice informaţii şi comunicări referitoare la prelucrarea datelor cu caracter personal, sunt uşor accesibile şi uşor de înţeles. Drept urmare, **persoana vizată trebuie informată cu privire la modul în care sunt prelucrate datele sale, într-o formă concisă, transparentă, inteligibilă şi accesibilă.**

Operatorul, poate colecta datele cu caracter personal, direct de la persoana vizată sau ele pot fi obţinute din alte surse.

1. **Informaţii care se furnizează persoanei vizate**, în momentul obţinerii datelor cu caracter personal, **în cazul în care acestea sunt colectate direct de la persoana vizată şi aceasta nu deţine deja informaţiile respective** (art. 13 alin (1), (2) şi (4) din Regulamentul (UE) 679 / 2016):
2. identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
3. datele de contact ale responsabilului cu protecţia datelor, după caz;
4. scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
5. interesele legitime urmărite de operator sau de o parte terţă, în cazul în care prelucrarea se face în temeiul art. 6 alin. (1) litera (f) din Regulamentul (UE) 679 / 2016;
6. destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
7. intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională, dacă este cazul;
8. perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
9. modalitatea în care persoana vizată îşi poate exercita drepturile;
10. atunci când prelucrarea se bazează pe art. 6 alin. (1) lit. (a) sau pe art. 9 alin. (2) lit. (a) din Regulamentul (UE) 679 / 2016, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
11. dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
12. dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;
13. existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la art. 22 alin. (1) şi (4), precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

1. **Informaţii care se furnizează persoanei vizate** (într-un termen rezonabil după obţinerea datelor cu caracter personal, dar nu mai mare de o lună), **în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată şi aceasta nu deţine deja informaţiile respective** (art. 14 alin (1), (2), (3) şi (5) din Regulamentul (UE) 679 / 2016):
2. identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
3. datele de contact ale responsabilului cu protecţia datelor, după caz;
4. scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
5. categoriile de date cu caracter personal vizate;
6. destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

7. intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională, dacă este cazul;
8. perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
9. interesele legitime urmărite de operator sau de o parte terţă, în cazul în care prelucrarea se face în temeiul art. 6 alin. (1) lit. (f) din Regulamentul (UE) 679 / 2016;
10. modalitatea în care persoana vizată îşi poate exercita drepturile;
11. atunci când prelucrarea se bazează pe art. 6 alin. (1) lit. (a) sau pe art. 9 alin. (2) lit. (a) din Regulamentul (UE) 679 / 2016, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
12. dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
13. sursa din care provin datele cu caracter personal şi, dacă este cazul, dacă acestea provin din surse disponibile public;
14. existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la art. 22 alin. (1) şi (4), precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

Art. 4. Minimizarea / Reducerea la minimum a datelor

Înainte de a procesa date cu caracter personal, trebuie să determinaţi:

1. dacă şi în ce măsură prelucrarea datelor cu caracter personal este necesară pentru atingerea scopului pentru care este efectuată;
2. tipul datelor cu caracter personal necesare, pentru realizarea procesului de prelucrare.

Datele cu caracter personal trebuie sa fie, cele mai adecvate, relevante şi strict limitate la ceea ce este absolut necesar, în raport cu scopurile în care sunt prelucrate.

Acolo unde scopul permite şi unde cheltuielile implicate sunt proporţionale cu obiectivul, trebuie folosite date anonime. Datele personale nu pot fi colectate în avans şi stocate în scopuri potenţiale viitoare, cu excepţia cazului în care acest lucru este impus sau permis de legislaţia naţională.

Art. 5. Limitarea stocării şi ştergerea

Datele cu caracter personal trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. Datele cu caracter personal care nu mai sunt necesare după expirarea procesului legal sau de afaceri, trebuie şterse/distruse/anonimizate. Pot exista situaţii în care interesele legale obligă la păstrarea acestor date pe termene predefinite. În acest caz, datele trebuie păstrate în dosare, până la expirarea obligaţiilor legale.

Art. 6. Exactitatea si actualitatea datelor

Datele cu caracter personal colectate trebuie să fie corecte, complete şi, dacă este necesar, să fie actualizate. Trebuie luate măsuri permanent pentru a ne asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere.

Art. 7. Integritate și confidențialitate

În cadrul MAZARINE ENERGY ROMANIA S.R.L., datele cu caracter personal sunt considerate informații confidențiale și trebuie protejate prin măsuri organizatorice și tehnice adecvate, pentru a preveni accesul neautorizat, prelucrarea sau distribuirea ilegală, precum și pierderea accidentală, modificarea sau distrugerea lor. Orice încălcare sau nerespectare a prezentei Politici sau a instrucțiunilor derivate din aceasta, în special, orice divulgare deliberată de date cu caracter personal către o persoană neautorizată sau terță parte, poate duce la sancțiuni disciplinare.

Nerespectarea acestui principiu, expune direct la breșe de securitate și confidențialitate și, implicit, la penalitățile extrem de severe prevăzute de Regulamentul (UE) 679 / 2016.

Operatorul este responsabil de respectarea principiilor Regulamentului (UE) 679 / 2016 și trebuie să poată demonstra conformitatea cu acestea („responsabilitate").

Capitolul 6

Prelucrarea datelor cu caracter personal

MAZARINE ENERGY ROMANIA S.R.L., colectează, utilizează, prelucrează și furnizează datele cu caracter personal oferite, numai pentru realizarea scopurilor în care acestea au fost colectate.

Prezenta Politică, stabilește datele cu caracter personal prelucrate de către Societate, în cadrul activităților desfășurate, astfel:

A) Datele cu caracter personal ale clienților și partenerilor

Art. 1 Prelucrarea datelor pentru o relație contractuală

Datele cu caracter personal ale potențialilor clienți, clienți existenți și parteneri, pot fi procesate în scopul de a încheia, de a executa și de a finaliza un contract. Aceasta include, de asemenea, servicii de consultanță pentru partener, în cazul în care, acest lucru are legătură cu scopul contractual. Anterior unui contract, în timpul fazei de inițiere a acestuia, datele cu caracter personal pot fi procesate, pentru a pregăti oferte sau alte documente care să îndeplinească diferite solicitări ale perspectivei legate de încheierea contractului. Persoanele pot fi contactate în timpul procesului de pregătire a contractului, folosind informațiile personale pe care acestea le-au furnizat. Orice restricții solicitate de potențialii client, trebuie să fie respectate.

Art. 2 Prelucrarea datelor în scop publicitar

Dacă persoana vizată contactează MAZARINE ENERGY ROMANIA S.R.L. pentru a solicita informații (de ex., să primească materiale informative despre oferte, promoții etc.), prelucrarea datelor pentru a răspunde acestei solicitări, este permisă.

Acțiunile de publicitate fac obiectul unor cerințe legale suplimentare. Datele personale pot fi prelucrate în scopuri publicitare, de cercetare a pieței și a opiniei publice, cu condiția ca această prelucrare să se realizeze în concordanță cu scopul pentru care datele au fost colectate inițial. Subiectul (persoana vizată) deținător al datelor, trebuie să fie informat cu privire la utilizarea datelor sale în scopuri publicitare. Dacă datele sunt colectate numai în scopuri publicitare, divulgarea de la persoana vizată este voluntară. Persoana vizată trebuie informată asupra faptului că, furnizarea datelor personale pentru prelucrarea în scopuri publicitare este voluntară și că, trebuie să se obțină un consimțământ din partea persoanei vizate, pentru a procesa datele respective în scopuri publicitare. Atunci când se acordă consimțământul, persoana vizată ar trebui să aibă posibilitatea de a alege între formele disponibile, cum ar fi, formulare predefinite tipărite, transmiterea consimțământului prin e-mail etc.

Dacă persoana vizată refuză utilizarea datelor sale în scopuri publicitare, datele acesteia nu mai pot fi utilizate și trebuie să fie blocate/șterse/restricționate pentru utilizarea în aceste scopuri.

Art. 3 Prelucrarea datelor pe baza consimțământului

Consimţământul persoanei vizate, înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate, prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc, să fie prelucrate.

Datele pot fi procesate, conform consimțământului persoanei vizate. Înainte de a-şi acorda consimţământul, persoana vizată trebuie să fie informată, în conformitate cu prevederile Cap. 5 art. 3. Declaraţia de aprobare – consimţământul, trebuie obţinută în scris sau în format electronic şi păstrat în scopul documentării. În cazul în care, prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a acordat consimţământul pentru prelucrarea datelor sale cu caracter personal.

Persoana vizată, are dreptul să îşi retragă în orice moment consimţământul. **Retragerea consimţământului**, nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimţământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca şi acordarea acestuia.

Prelucrarea datelor cu caracter personal ale unui copil, este legală, dacă copilul are cel puţin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală, numai dacă şi în măsura în care, consimţământul respectiv este acordat sau autorizat de titularul răspunderii părinteşti asupra copilului.

Art. 4 Prelucrarea datelor cu caracter special

Datele cu caracter personal sensibile, pot fi procesate numai dacă legea impune acest lucru sau persoana vizată

și-a dat acordul expres (consimțământul). Aceste date pot fi, de asemenea, prelucrate numai dacă este obligatoriu pentru îndeplinirea, exercitarea sau apărarea revendicărilor legale referitoare la persoana vizată. Dacă există intenția de a procesa datele sensibile, Responsabilul pentru protecția datelor cu caracter personal trebuie să fie informat în prealabil.

Art. 5 Procese decizionale individuale automatizate

Procesul decizional exclusiv automatizat, are loc, atunci când se iau decizii în privința unei persoane, prin mijloace tehnologice și fără nicio implicare umană. Aceste decizii se pot lua chiar și fără crearea de profiluri.

Deciziile automatizate, se pot baza pe orice tip de date, de exemplu:

- date furnizate în mod direct de persoanele în cauză (cum ar fi, răspunsurile la un chestionar);
- date observate în legătură cu persoane (cum ar fi, datele despre locație, colectate prin intermediul unei aplicații);
- date derivate sau obținute prin inferență, cum ar fi un profil deja creat al persoanei (de exemplu, un punctaj de bonitate).

Persoana vizată, are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar, într-o masură semnificativă. Decizia nu trebuie sa aibă la bază date sensibile.

Nu se aplică în cazul în care:

- decizia este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;
- decizia are la bază consimțământul explicit al persoanei vizate;
- „operatorul de date pune în aplicare măsuri corespunzatoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia";
- decizia este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului și care prevede, de asemenea, măsuri corespunzatoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

Art. 6 Prelucrarea datelor utilizatorilor site-ului web www.mazarine-energy.com

Pentru site-ul www.mazarine-energy.com, domeniile și subdomeniile acestuia, acolo unde sunt colectate, prelucrate și utilizate date cu caracter personal, persoanele vizate trebuie să fie informate despre acest lucru, într-o Notă de informare și, în cazul în care, site-ul folosește cookie-uri, persoanele vizate trebuie sa aibă acces la Politica de cookie-uri. Nota de informare și orice informații despre cookie-uri trebuie integrate, astfel încât, să fie ușor de identificat, direct accesibile și disponibile în mod constant persoanelor vizate.

Dacă sunt create profiluri de utilizare (urmărire) pentru a evalua utilizarea site-urilor web și a aplicațiilor, persoanele vizate trebuie să fie întotdeauna informate în mod corespunzător în nota de informare.

În cazul în care, pentru utilizatorii înregistrați, sunt utilizate date cu caracter personal, pentru identificarea și autentificarea persoanei vizate, se instituie măsuri de protecție suficiente în timpul accesului.

B) Datele cu caracter personal ale angajatului

Art. 1 Prelucrarea datelor pentru relația de muncă

În relațiile de muncă, datele cu caracter personal pot fi procesate dacă este necesar, pentru a iniția, efectua și a încheia contractul individual de muncă, precum și, pentru îndeplinirea obligațiilor legale care îi revin operatorului. La inițierea unei relații de muncă, datele cu caracter personal ale solicitanților, pot fi procesate. **În momentul în care se decide încheierea unui contract de muncă, odată cu solicitarea unui set de date personale și documente, se va efectua și informarea salariatului, cu privire la prelucrarea datelor cu caracter personal ale angajaților MAZARINE ENERGY ROMANIA S.R.L., în activitatea de Resurse Umane.**

În cazul în care, candidatul este respins, datele sale trebuie să fie șterse (în conformitate cu perioada de păstrare necesară), cu excepția cazului în care, solicitantul a fost de acord ca datele sale să rămână în dosar pentru un viitor proces de selecție. De asemenea, este necesar să se acorde consimțământul pentru a utiliza datele, atunci când se dorește continuarea proceselor de aplicare.

Totodată, în contextul relațiilor de muncă, în conformitate cu art. 5 din legea nr. 190 / 2018, privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679, în cazul în care, **sunt utilizate sisteme de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video la locul de muncă**, prelucrarea datelor cu caracter personal ale angajaților, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

- interesele legitime urmărite de angajator, sunt temeinic justificate și prevalează asupra intereselor sau drepturilor și libertăților persoanelor vizate;
- angajatorul a realizat informarea prealabilă obligatorie, completă și în mod explicit a angajaților;
- angajatorul a consultat sindicatul sau, după caz, reprezentanții angajaților, înainte de introducerea sistemelor de monitorizare;
- alte forme și modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator, nu și-au dovedit anterior eficiența;
- durata de stocare a datelor cu caracter personal este proporțională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate;
- afișarea pictogramei de informare, cu privire la zona supravegheată video.

Art. 2 Prelucrarea unui număr de identificare național

Număr de identificare național – numărul prin care se identifică o persoană fizică în anumite sisteme de evidență și care are aplicabilitate generală, cum ar fi: codul numeric personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială de sănătate.

Conform art. 4 din legea nr. 190 / 2018, prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, se poate efectua în situațiile prevazute de art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, în scopul prevăzut la art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679, respectiv al realizării intereselor legitime urmărite de operator sau de o parte terță, se efectuează cu instituirea de către operator a următoarelor garanții:

- punerea în aplicare de măsuri tehnice și organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum și pentru asigurarea securității și confidențialității prelucrărilor de date cu caracter personal, conform dispozițiilor art. 32 din Regulamentul (UE) 2016/679;
- stabilirea de termene de stocare în funcție de natura datelor și scopul prelucrării, precum și de termene specifice în care datele cu caracter personal trebuie șterse sau revizuite, în vederea ștergerii;
- instruirea periodică, cu privire la obligațiile ce le revin persoanelor care, sub directa autoritate a operatorului, prelucrează date cu caracter personal.

În raportul de muncă existent, scopul prelucrării datelor cu caracter personal, trebuie să se coreleze întotdeauna cu scopul contractului individual de muncă.

Art. 3 Prelucrarea datelor cu caracter special

Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Nu se aplică în urmatoarele situații:

1. a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal, pentru unul sau mai multe scopuri specifice;
2. b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate, în domeniul ocupării forței de munca și al securității sociale și protecției sociale, în masura în care, acest lucru este autorizat de dreptul Uniunii, de dreptul intern sau de un acord colectiv de muncă;
3. c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice;
4. d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate, de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legatură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;
5. e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod voluntar de către persoana vizata;
6. f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță;

7. g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern;
8. h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic, de furnizarea de asistență medicală / socială sau a unui tratament sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență social;
9. i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi: protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale;
10. j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.

Datele menționate anterior, pot fi prelucrate în scopurile menționate la litera (h), în cazul în care, datele respective sunt prelucrate de către un profesionist, supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate, în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente. **Categoriile de date cu caracter special, necesită un nivel ridicat de protecție.**

Art. 4 Procese decizionale individuale automatizate

Dacă, la un moment dat, datele cu caracter personal sunt prelucrate automat, ca parte a raporturilor de muncă și anumite date personale specifice sunt evaluate automat (de exemplu, în cadrul selecției personalului sau al evaluării profilurilor de competențe), această prelucrare automată nu poate constitui singura bază pentru deciziile care ar putea avea un impact negativ asupra angajatului respectiv. Pentru a evita deciziile eronate, procesul automatizat trebuie să fie asistat de o persoană fizică ce evaluează conținutul situației și această evaluare este baza deciziei. Persoana vizată trebuie, de asemenea, să fie informată despre faptele și rezultatele deciziilor individuale automatizate și despre posibilitatea de a răspunde.

Art. 5 Telecomunicații și internet

Echipamentele telefonice, adresele de e-mail, intranetul și internetul, împreună cu aplicațiile interne, sunt asigurate de companie, în interes de serviciu. Acestea sunt un instrument și o resursă a companiei, drept urmare, pot fi utilizate în cadrul reglementărilor legale aplicabile și al politicilor interne ale companiei. În cazul utilizării autorizate în scopuri personale, se va ține cont de prevederile Regulamentului și procedurilor interne și de legislația specifică privind telecomunicațiile.

Pentru asigurarea unui grad ridicat al securității informatice și în vederea soluționării incidentelor de securitate informatică, utilizarea echipamentelor telefonice, a adreselor de e-mail, a rețelelor intranet / internet și a rețelelor sociale interne, poate fi înregistrată, conform politicilor interne ale companiei. Evaluările acestor date, poate fi făcută în cazul în care, există suspiciuni de breșe de securitate, încălcări ale legilor în vigoare sau ale politicilor Societății, în interesul legitim al Operatorului. Aceste evaluări, pot fi efectuate, cu respectarea

principiului proporţionalităţii. Legislaţia naţională relevantă, trebuie respectată în acelaşi mod ca şi regulamentele Societăţii.

Pentru protejarea împotriva atacurilor asupra infrastructurii IT sau a utilizatorilor individuali, pot fi implementate măsuri de protecţie pentru conexiunile la reţeaua MAZARINE ENERGY ROMANIA S.R.L., care blochează conţinutul dăunător din punct de vedere tehnic sau care analizează modelele de atac.

Capitolul 7

Prelucrarea datelor cu caracter personal în baza unui interes legitim

Datele cu caracter personal pot fi, de asemenea, prelucrate în cazul în care este necesar să se susţină un interes legitim al MAZARINE ENERGY ROMANIA S.R.L.., însă, interesele legitime ale unui operator, pot constitui un temei juridic pentru prelucrare, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate.

În acest sens:

- Prelucrarea de date ce are drept scop marketingul direct, poate fi considerată ca fiind desfaşurată pentru un interes legitim.
- Prelucrarea datelor în măsura strict necesară şi proporţională în scopul asigurarii securităţii reţelelor şi a informaţiilor, constituie un interes legitim al operatorului de date în cauză.
- Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză.

Măsurile de control care necesită prelucrarea datelor angajatului, pot fi luate, numai dacă există o obligaţie legală de a face acest lucru sau există un motiv legitim. Chiar dacă există un motiv legitim, trebuie examinată întotdeauna proporţionalitatea măsurii de control. Interesele justificate ale companiei în aplicarea măsurilor de control (de exemplu, respectarea dispoziţiilor legale şi a normelor si regulamentelor interne ale companiei), trebuie să fie cântărite faţă de orice interese ale angajatului, care trebuie să fie protejate, astfel încât măsurile de control sa fie adecvate.

Pentru a putea recurge la interes legitim drept temei pentru prelucrare, organizaţia ar trebui să efectueze un test de echilibrare, pentru a determina dacă interesele sale, prevalează asupra drepturilor şi intereselor persoanei vizate.

Elemente care înclină balanţa în favoarea interesului legitim al operatorului, pot fi:

- Natura interesului (drept fundamental, interes public, interes comercial);

- Eventualul prejudiciu suferit de operator, dacă prelucrarea nu are loc;
- Prelucrarea implică un grup restrâns de persoane;
- Datele nu sunt dezvăluite către terți;
- Organizația nu are o poziție dominantă pe piață;
- Nu se prelucrează categorii de date speciale;
- Nu există un impact semnificativ asupra drepturilor persoanei vizate;
- Persoana vizată se poate aștepta, în mod rezonabil, la existența prelucrării.

Capitolul 8

Transferul datelor cu caracter personal

Transmiterea datelor cu caracter personal către destinatarii din afara sau din interiorul MAZARINE ENERGY ROMANIA S.R.L., este supusă cerințelor de autorizare pentru prelucrarea datelor cu caracter personal, în conformitate cu prevederile legale. Beneficiarul datelor, trebuie să utilizeze datele cu caracter personal, numai în scopurile definite.

Conform Comisiei Europene, transferurile de date în afara Uniunii Europene / SEE, sunt posibile doar:

- Către un stat căruia Comisia Europeană i-a recunoscut un nivel de protecție adecvat (Andora, Argentina, Canada, Elveția, Insulele Feroe, Guernsey, Israel, Insula Man, Japonia, Jersey, Uruguay si Noua Zeelanda); sau
- Daca transferul are loc în baza unor garanții adecvate.

Transferul în baza oricăruia dintre temeiurile de mai sus, nu necesită vreo aprobare / autorizare din partea Comisiei Europene sau a Autorității de supraveghere. Regulamentul General pentru Protectia Datelor prevede că, sunt supuse acelorași reguli și transferurile ulterioare (onward transfers).

În cazul transferului de date cu caracter personal către țări terțe (toate națiunile din afara Uniunii Europene / SEE) sau organizații internaționale, Compania și angajații săi, se obligă ca transferul de date cu caracter personal către acestea, să se facă doar după ce s-au prezentat din partea acestora, garanții adecvate, astfel cum sunt ele menționate în art. 46 alin. (2) din Regulamentul (UE) 679/2016, respectiv:

1. un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;
2. reguli corporatiste obligatorii, în conformitate cu art. 47 din Regulamentul (UE) 679/2016;
3. clauze standard de protecție a datelor adoptate de Comisie, în conformitate cu procedura de examinare menționată la art. 93 alin. (2) din Regulamentul (UE) 679/2016;
4. clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie, în conformitate cu procedura de examinare menționată la art. 93 alin. (2) din Regulamentul (UE) 679/2016 ;

5. codul de conduită aprobat în conformitate cu art. 40 din Regulamentul (UE) 679/2016, însotit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță, de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau
6. un mecanism de certificare aprobat, în conformitate cu art. 42, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță, de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

Sub rezerva autorizării din partea autorității de supraveghere competente, garanțiile adecvate, pot fi furnizate de asemenea, în special, prin:

1. clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională; sau
2. dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

Scutul de confidențialitate UE — SUA

Conform Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, în cadrul Plenarei Comitetului European pentru Protecția Datelor, desfășurată on-line în data de 17 iulie 2020, a fost adoptată **Declarația privind invalidarea de către Curtea de Justiție a Uniunii Europene a Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA.**

În atare situație, în absența unei decizii privind caracterul adecvat în temeiul art. 45 alin. (3) din Regulamentul (UE) 2016/679, transferul de date cu caracter personal către Statele Unite poate fi efectuat în conformitate cu unul din următoarele instrumente prevăzute de art. 46 din Regulamentul (UE) 2016/679:

- clauze standard de protecție a datelor,
- reguli corporatiste obligatorii,
- coduri de conduită și mecanisme de certificare.

De asemenea, transferul de date cu caracter personal către Statele Unite se poate realiza în temeiul derogărilor prevăzute la art. 49 din Regulamentul (UE) 2016/679.

Capitolul 9

Prelucrarea datelor privind contractele

MAZARINE ENERGY ROMANIA S.R.L., identifică relația cu partenerii de afaceri, nu per ansamblu, ci pe tipuri de operațiuni de prelucrare. O entitate, nu poate fi și operator și persoana împuternicită de operator, pentru aceeași operațiune de prelucrare.

- **În cazul relației de tipul operator – operator, prelucrarea datelor printr-un furnizor de produse / prestator de servicii, se va efectua cu obligativitatea încheierii unui Acord privind prelucrarea datelor cu caracter personal, care va cuprinde, cel puțin următoarele:**
- Datele de identificare ale operatorilor;
- Obiectul și durata prelucrării;
- Natura și scopul prelucrării;
- Tipul de date cu caracter personal prelucrate;
- Categoriile de persoane vizate;
- Obligațiile și drepturile operatorului;
- Drepturile persoanei vizate;
- Datele de contact ale Responsabililor cu protecția datelor cu caracter personal.

- **În cazul relației de tipul operator – persoană împuternicită de operator** (persoana fizică sau juridică, autoritatea publică, agenția sau alt organism, care prelucreaza datele cu caracter personal în numele operatorului)**, operațiunile de prelucrare de date cu caracter personal pe care le presupune colaborarea dintre cele doua părți, se va efectua cu obligativitatea încheierii unui Acord privind prelucrarea datelor cu caracter personal**, care va cuprinde, cel puțin următoarele:

- Datele de identificare ale operatorilor;
- Obiectul și durata prelucrării;
- Natura și scopul prelucrării;
- Tipul de date cu caracter personal prelucrate;
- Categoriile de persoane vizate;
- Obligațiile și drepturile operatorului;
- Drepturile persoanei vizate;
- Măsuri tehnice și organizatorice pentru asigurarea securității datelor cu caracter personal;
- Datele de contact ale Responsabililor cu protecția datelor cu caracter personal;
- **Instrucțiuni scrise ale operatorului.**

Acest Acord de Prelucrare a Datelor cu Caracter Personal trebuie sa fie documentat în formă scrisă, pe orice suport și constituie anexa la contractele existente sau contractele noi.

Pentru persoana împuternicită de operator, Acordul reprezintă actul care puncteaza instrucțiunile precise pe care le transmite operatorul și care definește, astfel, rolul și responsabilitățile fiecăreia dintre părți, cu respectarea prevederilor art. 28 (3) și (4) din Regulamentul (UE) 679 / 2016.

Persoana împuternicită de operator, trebuie să acționeze numai pe baza instrucțiunilor scrise ale operatorului (cu excepția cazului în care legea solicită să acționeze fără astfel de instrucțiuni). Instrucțiunile

operatorului, sunt acele explicaţii şi solicitări, care îl ajută pe împuternicit să ştie în orice moment ce are de făcut, fără să fie nevoie să ia el decizii în această privinţă. Persoana împuternicită de operator, nu ar trebui să ia niciun fel de decizie cu privire la prelucrările pe care le face în numele operatorului.

Operatorul recurge doar la persoane împuternicite care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât, prelucrarea să respecte cerinţele prevăzute în Regulamentul (UE) 679 / 2016 şi să asigure protecţia drepturilor persoanelor vizate.

Acordul de Prelucrare a Datelor cu Caracter Personal, pentru persoana împuternicită de operator, stabileşte următoarele:

1. prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respective interzice o astfel de notificare din motive importante legate de interesul public;
2. se asigură că persoanele autorizate să prelucreze datele cu caracter personal, s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;
3. adoptă toate măsurile necesare privind asigurarea securităţii prelucrării datelor, conform art. 32 din Regulamentul (UE) 679/2016;
4. persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizaţie scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizaţii generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecţii faţă de aceste modificări;
5. în cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activităţi de prelucrare specifice în numele operatorului, aceleaşi obligaţii privind protecţia datelor prevăzute în contractul sau în alt act juridic încheiat între operator şi persoana împuternicită de operator, astfel cum se prevede la art. 28 alin. (3) din Regulamentul (UE) 679/2016, revin celei de a doua personae împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerinţele regulamentului. În cazul în care această a doua persoană împuternicită nu îşi respectă obligaţiile privind protecţia datelor, persoana împuternicită iniţială rămâne pe deplin răspunzătoare faţă de operator în ceea ce priveşte îndeplinirea obligaţiilor acestei a doua persoane împuternicite;
6. oferă asistenţă operatorului, prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor sale;
7. ajută operatorul să asigure respectarea obligaţiilor prevăzute la art. 32-36 din Regulamentul (UE) 679/2016, ţinând seama de caracterul prelucrării şi informaţiile aflate la dispoziţia persoanei împuternicite de operator;
8. la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal, după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care, dreptul Uniunii sau dreptul intern impune stocarea acestora;
9. permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator;

10. în cazul procesării transfrontaliere a datelor din contracte, trebuie îndeplinite cerinţele Regulamentului (UE) 679/2016 şi a legislaţiei naţionale relevante, privind divulgarea datelor cu caracter personal în străinătate. În special, datele cu caracter personal din Spaţiul Economic European (SEE), pot fi procesate într-o ţară terţă din afara SEE, numai dacă partenerul poate dovedi că dispune de un standard de protecţie a datelor echivalent cu această politică de protecţie a datelor. Instrumentele adecvate pot fi:

- Acordul privind clauzele contractuale standard ale UE pentru prelucrarea datelor din contracte în ţările terţe cu furnizorul/prestatorul şi cu orice subcontractanţi;
- Participarea furnizorului/prestatorului la un sistem de certificare acreditat de UE, pentru asigurarea unui nivel suficient de protecţie a datelor;
- Recunoaşterea regulilor corporative obligatorii ale furnizorului/prestatorului, pentru a crea un nivel adecvat de protecţie a datelor, de către autorităţile de supraveghere responsabile pentru protecţia datelor.

Persoana împuternicită de operator, înştiinţează operatorul fără întârzieri nejustificate, după ce ia cunoştinţă de o încălcare a securităţii datelor cu caracter personal, pentru ca acesta să poată notifica acest lucru autorităţii de supraveghere competente, fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta.

Operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse.

Capitolul 10

Evidenţa activităţilor de prelucrare (Cartografierea)

Conform art. 30, alin. (1) din Regulamentul (UE) 679/2016, fiecare operator şi, după caz, reprezentantul acestuia, păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea lor.

Inventarierea datelor cu caracter personal, reprezintă procesul de localizare şi identificare al datelor cu caracter personal, în cadrul activităţii specifice a operatorului de date, realizându-se astfel, cartografierea datelor cu caracter personal.

Pentru a evalua în mod eficient impactul Regulamentului (UE) 679/2016 asupra activităţii Societăţii, este necesară identificarea prelucrărilor de date cu caracter personal efectuate şi păstrarea evidenţei activităţilor de prelucrare.

În acest sens, trebuie identificate, cu precizie, cel puţin următoarele:

- categoriile de date cu caracter personal / special prelucrate;
- scopurile urmărite prin operațiunile de prelucrare a datelor;
- temeiul legal al prelucrării;
- categoriile de persoane vizate;
- persoanele care au acces la aceste date;
- perioada de stocare a datelor prelucrate;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal;
- transferurile de date cu caracter personal către o țară terță sau o organizație internațională;
- modalitatea de asigurare a securității datelor prelucrate.

Menținerea unei înregistrări a activităților de prelucrare a datelor cu caracter personal, nu este o întreprindere singulară, ci un exercițiu permanent. Registrul de evidență a activităților de prelucrare, trebuie actualizat de câte ori este necesar, cu informarea prealabilă a DPO, cu privire la modificările ce urmează a fi efectuate. În acest sens, trebuie efectuate periodic, recenzii ale datelor prelucrate, pentru a ne asigura că documentația rămâne corectă și actualizată.

Fiecare Departament este direct răspunzător, atât cu privire la exactitatea datelor din Registrul de evidență a activităților de prelucrare, cât și cu actualizarea permanentă a acestuia.

Capitolul 11

Gestionarea riscurilor

În cazul în care, au fost identificate prelucrări de date cu caracter personal susceptibile de a prezenta **riscuri ridicate** pentru drepturile și libertățile persoanelor fizice, operatorul va efectua o **evaluare a impactului asupra protecției datelor (DPIA – Data Protection Impact Assessment)**, în condițiile art. 35 din Regulamentul General privind Protecția Datelor.

Evaluarea impactului asupra protecției datelor se realizează **anterior colectării** datelor cu caracter personal și efectuării prelucrării.

Se va pune accent pe **estimarea riscurilor asupra protecției datelor din punctul de vedere al persoanelor vizate, luând în considerare natura datelor, domeniul de aplicare, contextul și scopurile prelucrării și utilizarea noilor tehnologii.**

Evaluarea impactului asupra protecției datelor presupune:

- o descriere a prelucrării de date efectuate și a scopurilor acesteia;
- o evaluare a necesității și a proporționalității prelucrării de date efectuate;
- o estimare a riscurilor asupra drepturilor și libertăților persoanelor vizate;
- măsurile prevăzute pentru a trata riscurile și a asigura conformitatea cu dispozițiile RGPD.

Evaluarea impactului asupra protecţiei datelor permite:

- realizarea unei prelucrări de date cu caracter personal sau a unui produs care respectă viaţa privată;
- estimarea impactului asupra vieţii private a persoanelor vizate;
- demonstrarea faptului că principiile fundamentale ale Regulamentul General privind Protecţia Datelor, sunt respectate.

Evaluarea impactului asupra protecţiei datelor se impune, mai ales, în cazul:

(a) unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, menţionată la articolul 9 alineatul (1) din Regulament sau a unor date cu caracter personal privind condamnări penale şi infracţiuni, menţionată la articolul 10; sau

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

Când evaluarea de impact indică riscuri ridicate, în absenţa unor măsuri luate de operator pentru atenuarea acestora, se consultă Autoritatea naţională de supraveghere.

Capitolul 12

Iniţierea unui nou proces de prelucrare

Conform art. 25 din Regulamentul (UE) 679/2016, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât şi în cel al prelucrării în sine, pune în aplicare măsuri tehnice şi organizatorice adecvate. Pentru a fi în măsură să demonstreze conformitatea cu Regulamentul, operatorul trebuie să pună în aplicare măsuri, care să respecte în special principiul protecţiei datelor începând cu momentul conceperii, dar şi cel al protecţiei implicite a datelor.

În esenţă, acest lucru înseamnă că, operatorul trebuie să integreze protecţia datelor, atât la iniţierea şi implementarea sistemelor, serviciilor, produselor şi practicilor de afaceri care implică activităţi de procesare a datelor cu caracter personal, cât şi pe parcursul întregului proces de dezvoltare a acestora. Integrarea protecţiei datelor în cazul iniţierii unui nou proces de prelucrare, asigură atât respectarea principiilor şi cerinţelor fundamentale ale Regulamentului (UE) 679/2016, cât şi anticiparea riscurilor şi a evenimentelor invazive, înainte de apariţia acestora.

Astfel de măsuri ar putea consta, printre altele, în:

- reducerea la minimum a prelucrării datelor cu caracter personal (realizată prin analizarea tipurilor de date cu caracter personal colectate și necesitatea prelucrării acestora);
- stabilirea perioadei de stocare a datelor prelucrate;
- stabilirea modalităților de distrugere a datelor, după expirarea perioadei de stocare;
- stabilirea entităților către care se divulgă datele cu caracter personal (destinatarii acestora);
- stabilirea măsurilor de securitate a datelor prelucrate;
- stabilirea persoanelor care au acces la datele cu caracter personal prelucrate.

În acest sens, în cazul inițierii unui nou proces de prelucrare a datelor cu caracter personal, este obligatorie consultarea Responsabilului cu protecția datelor cu caracter personal.

Capitolul 13

Drepturile persoanei vizate

Fiecare persoană vizată, are conform Regulamentului, drepturile detaliate în continuare, fiecare solicitare urmând să fie tratată de către Responsabilul cu protecția datelor cu caracter personal, cu obligația de a răspunde cererilor persoanei vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivelor cereri, să motiveze acest refuz.

Art.1. Dreptul de a fi informat – În cazul în care, datele cu caracter personal sunt obținute direct de la persoana vizată, MAZARINE ENERGY ROMANIA S.R.L., este obligată să furnizeze persoanei vizate, informațiile prezentate în Cap. V, art. 3, pct. 1 din prezenta Politică, cu excepția cazului în care, această persoană posedă deja informațiile respective. În cazul în care, datele cu caracter personal sunt obținute din alte surse, MAZARINE ENERGY ROMANIA S.R.L., este obligată să furnizeze persoanei vizate, informațiile prezentate în Cap. V, art. 3, pct. 2 din prezenta Politică, cu excepția cazului în care, această persoană posedă deja informațiile respective.

Art. 2. Dreptul de acces – MAZARINE ENERGY ROMANIA S.R.L. este obligată, în situația în care prelucrează date cu caracter personal care privesc solicitantul, să-i comunice acestuia, împreună cu confirmarea, cel puțin urmatoarele: a) informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le-au fost sau urmează să le fie divulgate datele, în special destinatari din țări terțe sau organizații internaționalele; b) comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum și a oricărei informații disponibile cu privire la originea datelor; c) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă; d) informații asupra principiilor de funcționare a mecanismului prin care se efectuează orice prelucrare automată a datelor care vizează persoana respectivă; e) informații privind existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării, precum și condițiile în care pot fi exercitate; f) informații asupra posibilității de a înainta plângere către autoritatea de supraveghere, precum și de a se adresa instanței pentru atacarea deciziilor operatorului, în conformitate cu dispozițiile legii;

Art. 3. Dreptul de intervenție asupra datelor – Orice persoană vizată, are dreptul de a obține de la MAZARINE ENERGY ROMANIA S.R.L., la cerere și în mod gratuit: a) după caz, rectificarea, actualizarea, blocarea sau ștergerea datelor a caror prelucrare nu este conformă legii, în special a datelor incomplete sau inexacte;

Art. 4. Dreptul de opoziție – Persoana vizată, are dreptul de a se opune în orice moment, din motive întemeiate și legitime, legate de situația sa particulară, ca date care o vizează, să facă obiectul unei prelucrări, cu excepția cazurilor în care, există dispoziții legale contrare. În caz de opoziție justificată, prelucrarea nu mai poate viza datele în cauză;

Art. 5. Dreptul de a nu fi supus unei decizii individuale – Orice persoană, are dreptul de a cere și de a obține retragerea/anularea/reevaluarea oricarei decizii care produce efecte juridice în privința sa, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalității sale, precum competența profesională, credibilitatea, comportamentul sau alte asemenea aspecte;

Art. 6. Dreptul de ștergere a datelor – Persoana vizată, are dreptul să solicite operatorului să șteargă fără întârziere, datele cu caracter personal care o privesc, în următoarele cazuri: a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate; b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare; c) persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea; d) datele cu caracter personal au fost prelucrate ilegal; e) datele cu carecter personal trebuie șterse pentru respectarea legii;

Art. 7. Dreptul la restricționarea prelucrării datelor – Conform art. 18 din Regulament, persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în următoarele cazuri: a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea acestora; b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor; c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță; d) persoana vizată s-a opus prelucrării în conformitate cu art. 21 alin. (1) din Regulament, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

În cazul în care prelucrarea a fost restricționată în baza situațiilor sus-menționate, astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

O persoană vizată care a obținut restricționarea prelucrării în baza situațiilor prezentate mai sus, este informată de către operator înainte de ridicarea restricției de prelucrare.

Art. 8. Dreptul la portabilitatea datelor – Art. 20 din Regulament, stipulează: Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului, într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului carui i-au fost furnizate datele cu caracter personal. Datele personale trebuie să poată fi oferite persoanei vizate, într-un format structurat, pentru ca aceasta să poată decide dacă le descarcă sau, dimpotrivă, dacă le poate trimite unui alt operator. Acest drept se aplică doar în masura în care datele sunt prelucrate în temeiul unui contract sau a consimțământului persoanei vizate, precum și (cumulat),

atunci când prelucrarea se face prin mijloace automate. Dreptul la portabilitatea datelor se aplică atât asupra datelor furnizate direct de persoana vizată, cât și asupra datelor colectate ulterior. Sunt excluse de la portabilitate, datele derivate sau deduse cu privire la persoanele vizate;

Art. 9. Dreptul de a depune o plângere – Persoana vizată are dreptul de a depune o plângere la Autoritatea Națională de Supraveghere a Protecției Datelor cu Caracter Personal (ANSPDCP) și de a se adresa instanței.

Toate aceste drepturi, pot fi exercitate de către persoana vizată, printr-o cerere scrisă, semnată și datată, transmisă la sediul Societății, cu mențiunea: „Responsabilului cu protecția datelor cu caracter personal" sau la următoarea adresă de e-mail: dpo.romania@mazarine.energy

Capitolul 14

Confidențialitatea procesării

Datele cu caracter personal, sunt considerate confidențiale. **Orice colectare, prelucrare sau utilizare neautorizată a acestor date de către angajați, este interzisă.** Șefii de serviciu, pot stabili nivelul de acces la date cu caracter personal, pentru fiecare subaltern. Orice procesare de date, efectuată de un angajat care nu a fost autorizat să o îndeplinească, ca parte a îndatoririlor sale legitime, este neautorizată. Se aplică principiul „necesității de a cunoaște – need to know". Angajații pot avea acces la date cu caracter personal, numai după cum este adecvat pentru tipul și scopul sarcinii de serviciu în cauză. Acest lucru, necesită o defalcare atentă și separarea, precum și punerea în aplicare a rolurilor și responsabilităților. **Angajaților li se interzice să utilizeze date cu caracter personal în scopuri private sau comerciale, să le dezvăluie persoanelor neautorizate sau să le pună la dispoziție în orice alt mod.** Departamentul Resurse Umane trebuie să-și informeze angajații, la începutul relației de muncă, cu privire la obligația de a proteja confidențialitatea datelor cu caracter personal și a informațiilor.

Responsabilitățile generale ale angajaților MAZARINE ENERGY ROMANIA S.R.L., în cadrul Regulamentului (UE) 679/2016 privind protecția datelor cu caracter personal, includ:

- de a prelucra datele cu caracter personal în conformitate cu, și în limitele atribuțiilor din fișa postului;
- de a păstra confidențialitatea asupra datelor cu caracter personal pe care le prelucrează, pe toată durata contractului individual de muncă și după încetarea acestuia, pe termen nelimitat;
- de a nu dezvalui datele cu caracter personal pe care le prelucrează, unor alte persoane decât cele în privința cărora îi este permis acest lucru prin procedurile interne, prin regulamentul intern al angajatorului, prin contractul individual de muncă și fișa postului;
- de a prelucra datale cu caracter personal, numai pentru aducerea la îndeplinire a atribuțiilor de serviciu prevazute in fișa postului, în contractul individual de muncă și în regulamentul intern;
- de a respecta masurile tehnice și organizatorice stabilite pentru protejarea datelor cu caracter personal, împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului

neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală;
- de a aduce la cunoştinţa Responsabilului cu protecţia datelor cu caracter personal, în cel mai scurt timp posibil, orice situaţie de acces neautorizat la datele personale pe care le prelucrează.

Nerespectarea obligaţiilor antemenţionate, precum şi a confidenţialităţii asupra datelor şi informaţiilor cu caracter personal prelucrate, atrage răspunderea disciplinară a salariatului, în conformitate cu prevederile legislaţiei muncii şi a legislaţiei în domeniul protecţiei datelor cu caracter personal.

Orice angajat al organizaţiei, are obligaţia de informa imediat Responsabilul cu protecţia datelor cu caracter personal, privind orice incident sau eveniment care afecteaza negativ confidenţialitatea, interigatea si diponibilitatea datelor sau care poate crea prejudicii organizaţiei.

Orice prejudiciu, de orice natură, adus organizaţiei cu sau fără intenţie, prin nerespectarea prevederilor legislaţiei şi Regulamentului, privind datele cu caracter personal, poate atrage răspunderea disciplinară sau civilă (după caz).

Capitolul 15

Securitatea prelucrării

Datele cu caracter personal, trebuie să fie protejate împotriva accesului neautorizat şi a prelucrării sau dezvăluirii ilegale, precum şi a pierderii, modificării sau distrugerii accidentale. Acest lucru se aplică, indiferent dacă datele sunt prelucrate electronic sau pe suport de hârtie.

Pentru îndeplinirea prevederilor legale aferente şi în vederea satisfacerii cerinţelor păstrarii în siguranţă a datelor şi informaţiilor, compania a elaborat şi implementat măsuri organizatorice şi tehnice, referitoare la securitatea şi controlul sistemelor informatice, în vederea asigurării confidenţialităţii datelor şi informaţiilor, precum şi pentru păstrarea în siguranţă a acestora, în cadrul activităţii curente, executate de angajaţii Societăţii.

Prelucrările manuale de date cu caracter personal:

- 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 dupa terminarea acestora.
- Prelucrările manuale de date cu caracter personal, care fac parte din categoria datelor cu carecter special sau sensibil, se vor efectua numai de către persoanele care au atribuţii specifice în acest sens.

Toate documentele care conţin date cu caracter personal urmează regulile de păstrare, procesare, multiplicare, transport, transmitere, distrugere şi arhivare, stabilite prin legislaţia în domeniul formării profesionale, legea

arhivării, legislația în domeniul contabilității, legislația muncii etc. și prin procedurile interne existente la nivelul MAZARINE ENERGY ROMANIA S.R.L.

Capitolul 16

Controlul prelucrării și protecției datelor cu caracter personal

Monitorizarea respectării Politicii de prelucrare și protecție a datelor cu caracter personal și a legilor aplicabile privind protecția datelor, este verificată în mod regulat prin intermediul auditurilor de protecție a datelor și al altor controale.

Efectuarea acestor controale revine Responsabilului cu Protecția Datelor cu Caracter Personal, conform art. 39 alin. (1) lit. b) din Regulamentul (UE) 679 / 2016. Rezultatele controalelor privind protecția datelor, trebuie raportate Managerului MAZARINE ENERGY ROMANIA S.R.L.

La cerere, rezultatele controalelor privind protecția datelor vor fi puse la dispoziția Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal.

Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal, poate efectua propriile controale, conform legislației naționale.

Capitolul 17

Incidente de Securitate

Incidentul de securitate poate fi definit astfel:

– ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrității, disponibilității, confidențialității informației de pe un sistem informatic automatizat sau la un sistem manual (orice document, pe suport de hârtie, care conține date cu caracter personal, și este accesat de persoane neautorizate);

– orice acțiune sau inacțiune contrară reglementărilor de securitate, ale cărei consecințe au determinat ori sunt de natură să determine, compromiterea securității datelor;

– orice tip de evenimente, în care există suspiciuni justificate, că datele cu caracter personal sunt capturate, colectate, modificate, copiate, transmise sau utilizate în mod ilegal. Aceasta se referă la acțiunile unor terți sau ale angajaților.

Un incident informatic, se poate referi la: examinarea neautorizată de inforrnații și date, întreruperea funționării unor servicii sau produse, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea neautorizata a informațiilor, modificarea informațiilor și datelor din sistemele informatice, malware sau software, cu sau fără știința sau intenția utilizatorului.

Informația se consideră compromisă, atunci când își pierde integritatea, confidențialitatea sau disponibilitatea.

Abaterea de la reglementările de securitate, reprezintă o încălcare a acestora, care conduce la o compromitere a informației.

Responsabilul cu protecția datelor cu caracter personal (DPO), răspunde în fața Conducerii, privind modul de tratare a incidentelor de Securitate, în raport cu ANSPDCP.

Tratarea incidentelor de securitate se aplică nediscriminatoriu, tuturor persoanelor care folosesc resursele informaționale ale organizației.

Raportarea incidentului de securitate care vizează compromiterea datelor cu caracter personal, trebuie să cuprindă:

- descrierea datelor compromise, data emiterii, emitentul, subiectul la care se referă, persoana sau compartimentul care le-a gestionat;
- o scurtă prezentare a împrejurărilor în care a avut loc compromiterea, inclusiv data constatării, perioada în care datele au fost expuse compromiterii, persoanele neautorizate care au avut sau ar fi putut avea acces la acestea, dacă sunt cunoscute;
- alte precizări cu privire la eventuala informare a emitentului.

În situația în care, incidentul de securitate implică aplicarea legilor civile sau penale, DPO va recomanda sesizarea organelor în drept ale statului și va acționa ca ofițer de legatură cu acestea.

Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt, în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse.

Orice incident de securitate care implică date cu caracter personal, se raportează imediat la DPO, de către orice angajat al organizației în care s-a produs compromiterea ancestors, astfel încât, să poată fi respectate toate obligațiile de raportare, în conformitate cu legislația națională.

Capitolul 18

Responsabilități și sancțiuni

Managerii de departament din cadrul Societății, sunt responsabili pentru prelucrarea datelor în zona lor de responsabilitate. Prin urmare, ei sunt obligați să se asigure că cerințele legale pentru protecția datelor și cele conținute în Politica de prelucrare a datelor cu caracter personal, sunt îndeplinite. Personalul de conducere este responsabil pentru asigurarea măsurilor organizatorice, tehnice și a celor care țin de resursele umane, pentru ca orice prelucrare a datelor cu caracter personal să se efectueze în conformitate cu REGULAMENTUL (UE) 2016 / 679. **Conformitatea cu aceste cerințe este responsabilitatea fiecărui angajat relevant.**

Responsabilul cu protecția datelor cu caracter personal, este persoana de contact pentru relații privind prelucrarea și protecția datelor. Acesta poate efectua verificări cu privire la respectarea Politicii de prelucrare a datelor cu caracter personal și a prevederilor Regulamentului (UE) 2016 / 679.

Toți angajații trebuie să informeze imediat Responsabilul cu protecția datelor cu caracter personal, cu privire la cazurile de încălcare a acestei Politici de protecție a datelor sau a altor reglementări privind protecția datelor cu caracter personal.

Departamentele responsabile cu proiectele de afaceri care implică procese de prelucrare majore, trebuie să informeze Responsabilul cu protecția datelor cu caracter personal în timp util, cu privire la o nouă prelucrare a datelor cu caracter personal. Pentru prelucrarea datelor care pot prezenta riscuri speciale pentru drepturile individuale ale persoanelor vizate, Responsabilul cu protecția datelor cu caracter personal trebuie să fie informat înainte de începerea procesării. Acest lucru este valabil în special la date personale extrem de sensibile.

Prelucrarea necorespunzătoare a datelor cu caracter personal sau alte încălcări ale legilor privind protecția datelor, conduce la suportarea sancțiunilor prevăzute de reglementările interne, de Regulamentul UE nr. 679/2016 și de legislația în vigoare.

Capitolul 19

Responsabilul cu protecția datelor cu caracter personal (DPO)

Responsabilul cu protecția datelor cu caracter personal, fiind independent intern de subordonarea profesională, activează în vederea respectării reglementărilor naționale și internaționale privind protecția datelor. El este responsabil pentru Politica de protecție a datelor și supraveghează respectarea acesteia și a

Regulamentului. Responsabilul cu protecția datelor cu caracter personal, este desemnat de conducerea MAZARINE ENERGY ROMANIA S.R.L.

Managerii de departament, au obligația să informeze cu promptitudine Responsabilul cu protecția datelor cu caracter personal, despre apariția oricăror riscuri cu privire la prelucrarea și protecția datelor personale (breșe de securitate).

Orice persoană vizată, se poate adresa Responsabilului cu protecția datelor cu caracter personal, în orice moment, pentru a pune întrebări, a solicita informații sau pentru a depune plângeri legate de protecția datelor sau de problemele de securitate a datelor personale. Dacă există solicitări, plângerile vor fi tratate în mod confidențial.

Dacă Responsabilul cu protecția datelor cu caracter personal nu poate soluționa o plângere sau remedia o încălcare a Politicii pentru protecția datelor, se va solicita consultanță la Autoritatea de supraveghere.

Deciziile luate de Responsabilul cu protecția datelor cu caracter personal pentru a remedia încălcările privind protecția datelor, trebuie să fie raportate către conducerea societății. Anchetele și controalele efectuate de Autoritatea de supraveghere, trebuie să fie întotdeauna raportate către conducerea companiei.

Responsabilul cu protecția datelor cu caracter personal (DPO), este proprietarul acestui document și este responsabil pentru revizia acestei politici, în conformitate cu cerințele interne.