Del Mar Energy Inc.

Del Mar Energy Inc.

4131 N Central Expressway, Suite 900, Dallas, Texas 75204
+1(940)2020502
Dallas

Personal Data Processing and Protection Policy of Del Mar Energy Inc. Terms and definitions

1.1. Personal Data: Information about an individual, such as name, date of birth, contact information, passport information, and income information used to identify them.

1.2. Special data categories: This is data that requires special protection, including information about health, race, biometric data, and criminal record information.

1.3. Data processing: Any action involving the collection, recording, systematization, storage, modification, use, transfer, depersonalization and destruction of data.

1.4. Personal data subject: An individual whose data is being processed, including employees, customers, partners, and contractors.

1.5. Data operator: An organization or person responsible for determining the purposes and methods of data processing.

1.6. Cross-border transfer: The movement of data outside the United States, in particular to countries that comply with international data protection standards.

1.7. Depersonalization of data: Transformation of data in such a way that it cannot be used to identify a subject.

1.8. Data confidentiality: Ensuring the safety of data, excluding unauthorized access and use.

1.9. Automated data processing: The use of information systems to process personal data without human intervention.

1.10. Personal Data Information system: An organized set of databases that provide automatic or manual data processing.

2. General positions

2.1. This Policy has been developed in accordance with the laws of the United States (Privacy Act, CCPA) and international standards GDPR.

2.2. The Policy regulates the collection, storage, use and destruction of data belonging to individuals.

2.3. The Company undertakes to ensure the rights of data subjects and protect their personal information from unauthorized use.

2.4. This Policy applies to all employees, partners, contractors, and customers who interact with Del Mar Energy Inc.

2.5. The Company is obliged to comply with the principles of legality, transparency and expediency of data processing.

2.6. The policy is mandatory for all employees of the company, regardless of their position.

2.7. Regular monitoring of compliance with the Policy is carried out by the company's internal auditors.

2.8. Changes in the Policy of data subjects are notified through the company's official website.

2.9. The Company reserves the right to update the Policy in case of changes in legislation or internal processes.

2.10. Violations of the Policy will result in disciplinary action or liability under U.S. law.

3. Principles and conditions of data processing

3.1. Legality: Data processing is carried out in strict accordance with legal norms and regulations.

3.2. Transparency: The Company informs the subjects about the purposes and methods of data processing, as well as provides access to their personal data upon request.

3.3. Intended use: Data is collected and processed solely for pre-defined purposes, such as fulfilling contracts or complying with regulatory requirements.

3.4. Minimization: The Company limits the amount of data collected, processing only those data that are necessary to achieve the purposes of processing.

3.5. Accuracy: Data is regularly updated and checked for relevance; errors or outdated information must be corrected.

3.6. Retention period limitation: Personal Data is stored only for as long as it is necessary to fulfill the purposes of processing.

3.7. Security: The Company provides data protection through technical and organizational measures to prevent leakage or unauthorized access.

3.8. Confidentiality: Access to the data is provided only to authorized employees with the required security clearance.

3.9. Respect for the rights of data subjects: The Company respects the rights of subjects to access, correct, restrict or delete data.

3.10. Responsibility: Company employees are personally responsible for following the Policy in their professional activities.

4. Objectives, legal grounds, and categories of processed data

4.1. Data processing purposes:

- Management of labor relations with employees.Conclusion and execution of contracts with clients and partners.

- Compliance with regulatory and legislative requirements.

4.2. Legal grounds for processing:Consent of the data subject to processing.The need to fulfill contractual obligations.Requirements of the US legislation.

4.3. Categories of processed data: Personal information: name, contact information, date of birth. Financial information: bank details, tax data. Work data: qualifications, length of service, position.

4.4. Data collection: Is carried out only with the consent of the subject, except in cases stipulated by law.

4.5. Processing methods: Include both automated and manual procedures.

4.6. Special categories of data: Processed only with the consent of the subject or if there are legal grounds.

4.7. Depersonalization of data: Used to process large amounts of data for analytical purposes.

4.8. Data transfer: Is carried out within the limits of legislation and with strict observance of confidentiality principles.

4.9. Cross-border transfer: Allowed only to countries with an adequate level of data protection.

4.10. Termination of processing: Occurs after the achievement of the objectives or at the request of the subject.

5. Data processing procedures and security requirements

5.1. Data collection is carried out strictly with the consent of the subject, except in cases provided for by law.

5.2. All personal data is stored in secure databases using encryption methods.

5.3. The transfer of data to third parties is allowed only if there is a legal basis and confidentiality is respected.

5.4. Data retention periods are set depending on the purposes of their processing and legal requirements.

5.5. Data destruction is carried out using certified methods that exclude the possibility of recovery.

5.6. All transactions with personal data are documented and recorded in accounting logs.

5.7. Access to the data is provided only after authorization.

5.8. The company implements regular monitoring of systems to detect and prevent security threats.

5.9. All employees are trained in data processing and protection.

5.10. Violations of the data processing procedure are subject to internal investigation.

6. Confidentiality of data and transfer to third parties

6.1. All personal data processed by the company is classified as confidential information.

6.2. Access to the data is provided only to employees and third parties with appropriate authority.

6.3. The transfer of data to third parties is allowed only if there is a legal basis and the consent of the data subject, if required by law.

6.4. When transferring data to third parties, the company enters into confidentiality agreements with these parties.

6.5. The data may be transferred to regulatory authorities or government agencies only within the framework of US law.

6.6. Cross-border data transfer is carried out only to countries with an adequate level of personal data protection.

6.7. All cases of data transfer are documented in special accounting logs.

6.8. The Company conducts regular checks of the parties accessing the data for compliance with security standards.

6.9. Any data leak or breach of confidentiality is subject to immediate investigation.

6.10. Data subjects are informed about the transfer of their data to third parties within the time limits prescribed by law.

7. Personal data secure

7.1. The company uses encryption systems and other technical security measures to protect its data.

7.2. All information systems of the company are regularly checked for vulnerabilities.

7.3. The company implements multi-layered protection to prevent cyber attacks.

7.4. Access to data is limited to multi-factor authentication of employees.

7.5. Trainings for employees on information security issues are regularly conducted.

7.6. Backup copies of the data are installed to prevent their loss in case of incidents.

7.7. Any suspicious activity with the data is recorded and analyzed by the security department.

7.8. The company cooperates with external experts to assess the level of data security.

7.9. In the event of a data leak, subjects are informed within 72 hours, as required by U.S. law.

7.10. The company's information security policy is reviewed at least once a year.

8. The rights of data subjects

8.1. Data subjects have the right to receive information about how their data is processed.

8.2. Subjects can request access to their data stored in the company.

8.3. There is a right to correct inaccurate or outdated information.

8.4. Subjects have the right to request the deletion of data in cases prescribed by law (for example, when withdrawing consent).

8.5. Subjects may restrict the processing of their data if they believe that it is being used unlawfully.

8.6. The right to data portability has been established, if required by law.

8.7. Subjects can withdraw their consent to data processing at any time.

8.8. They also have the right to file a complaint with regulatory authorities in case of violations of their rights.

8.9. The Company is obliged to provide information about data processing to the subjects within 30 calendar days from the date of the request.

8.10. The rights of data subjects are fully respected, regardless of the purposes of processing.

9. The procedure for reviewing requests from data subjects

9.1. Data subjects can submit a request for access, correction or deletion of data through the company's official contact address.

9.2. Each request is registered in the company's request accounting system.

9.3. Requests are processed within a period not exceeding 30 calendar days.

9.4. In cases of complexity of data processing, the period may be extended up to 60 days, with notification of the data subject.

9.5. The company provides confirmation of receipt of the request within 5 business days.

9.6. Responses to requests are provided in written or electronic form, depending on the preferences of the subject.

9.7. In case of refusal to satisfy the request, the subject is provided with a justification for the refusal.

9.8. If the request is related to the transfer of data to third parties, the company is obliged to provide information about such persons.

9.9. All requests and their processing are documented for internal audit.

9.10. In case of violation of the rights of the subjects, the company is obliged to eliminate the mistakes made and compensate for the damage.

10. Responsibility and making changes to the Policy

10.1. Employees who violate the Policy are subject to disciplinary liability in accordance with the company's internal regulations.

10.2. In case of gross violations, administrative or civil liability is possible in accordance with US law.

10.3. Any violation of the Policy is recorded and becomes the subject of an internal investigation.

10.4. The Policy is reviewed annually or in case of legislative changes.

10.5. Changes to the Policy are approved by the company's management and take effect immediately.

10.6. The updated version of the Policy is published on the company's official website.

10.7. Data subjects are notified of significant Policy changes within 10 business days.

10.8. The policy applies to all employees, contractors, and partners of the company.

10.9. Changes to the Policy are made taking into account international standards and local legislation.

10.10. Policy violations may lead to a review of internal procedures and increased data protection measures.

Signatures of the parties
Company:
Del Mar Energy Inc.
Michael Latham
CEO