Data Protection and Processing Policy

IGDP_P2 VERSION 1.00

CONTENTS

ALADDIN MIDDLE EAST LTD – TURKEY ANKARA BRANCH OFFICE

DATA PROTECTION AND PROCESSING POLICY

Introduction

This Policy document constitutes the Aladdin Middle East Limited – Turkey Branch Office, having its registered office at the following address "Karum İş Merkezi İran Caddesi No:21/394 Kavaklıdere Çankaya/Ankara" (hereinafter referred as the "Company" or "AME Turkey") Data Protection and Processing Policy and aims to provide information relating to purposes for which we gather and process personal data pursuant to Law No 6698 on Personal Data Protection (hereinafter referred as "Law", how we protect, store, process, transfer, erase, take legal, technical and administrative measure for pseudonymisation and anonymization of data and comply with our duty of transparent information, communication and modalities for the exercise of the rights of the data subjects in accordance with Article 10 of the Law. Accordingly, the purposes for which our Company processes personal data, to whom and for what purposes the processed data can be transferred, our personal data collection methods and legal reasons and the rights of the data subject may be found below.

Data Controller : Aladdin Middle East Limited Şirketi - Türkiye Ankara Şubesi

Trade Registration Number:80527

Address :Karum İş Merkezi İran Caddesi No:21/394 Çankaya ANKARA

Telephone : (+90)0 312 427 90 20

E-Mail :kvkk@ame.com.tr

Web Site :ame.com.tr

Field of Activity : Crude Oil Drilling

1. PURPOSE AND SCOPE

1.1.Purpose and Scope of the Policy

AME aims to comply with the Law by creating all kinds of legal grounds and processes for the protection and processing of personal data through this "Data Protection and Processing Policy (" Policy ") and by creating awareness on this issue among all stakeholders we are associated with.

This policy applies to all Personal Data processed by the Company, regardless of the media on which that data is stored or whether it relates to past or present employees, workers, employees of organizations we cooperate with, customers, clients or supplier contacts, shareholders, website users or any other Data Subject whose personal data may be gathered, registered, stored, processed, used, transferred by our Company.

1.2.Enforcement and Amendment

This Policy has been established by the Company and shall enter into force on the date of its publication on the official website (s) of AME Turkey and made available to the relevant parties upon the request of the data subjects. In the event of a conflict between the provisions of this Policy and the provisions of legislation in force, especially the aforementioned Law, the provisions of the latter shall prevail.

The Company reserves the right to amend or modify this Policy without prior notice to reflect technological advancements, legal and regulatory changes and good business practices. Such changes and/or modifications shall become effective immediately upon the posting thereof to our website. Current version of the Policy is available at http://aladdinmiddleeast.com/TR.aspx

1.3.Data Subject Groups Covered by the Policy

This Policy contains statements and explanations regarding the processing of personal data of categories of real persons listed below by AME within the scope of the Law. In this context, the application area of the Policy is the processing of personal data belonging to the following data subjects:

DATA SUBJECT CATEGORIES	EXPLANATION
Employee/Intern Candidates:	It refers to real persons who have applied for a job to our company in any way or who have submitted their CV and related information to our company's consideration.
Previous Employees:	It refers to real persons whose employment contract with our company has terminated for any reason (resignation, dismissal, retirement, etc.).
Active Customers:	Natural persons whose personal data we may process as a result of contractual relationship with our company and within the scope of any business relationship with our company.
Potential Customers:	Real persons about whom our company has obtained their personal data within the scope of any business relationship without any contractual relationship with our company.
Company Employees:	It refers to persons working in the Company or organizations affiliated with the Company whose personal data are processed within the framework of activities such as human resources, audit, information technology security and provision of infrastructure, legal compliance etc.
Parties who have submitted Applications or Complaints:	It refers to real persons who transmit their opinions / complaints / suggestions or information and other requests to our Company, whether they have benefited from our Company's services or not.

Visitor:	It refers to real persons who visit our Company premises or other service sites, benefit from our company's guest internet network or visit our Company's website http://aladdinmiddleeast.com/TR.aspx.
Relatives of Data Subject:	Refers to individuals who are family members and relatives of our employees and / or employees who benefit from our company's services.
Parties to who we provide services:	It refers to real persons who benefit from the services offered by the Company in its fields of activity.
Employee/Representative/Shareholder of Contractors	It refers to real persons who are shareholders, representatives or employees of companies that provide goods and / or services to our Company based on the existing and / or prospective contracts signed with our Company.
Employee/Representative/Shareholder of Organizations that we collaborate	It refers to natural persons, including the shareholders and representatives of these institutions, working in the institutions with which the company has any business relationship (such as, but not limited to, business partners, suppliers)
Other 3rd Parties:	Any third party whose personal data may be processed by the Company that are not specifically mentioned in this Policy.

The categories of data subjects described above are for illustrative purposes. The fact that the data subject does not fall within the scope of any of these categories does not eliminate the data subject qualification as specified in the Law.

1.4.Definitions

For the purpose of this Directive the following definitions shall apply:

Company: Aladdin Middle East Limited Şirketi - Türkiye Ankara Şubesi,

Personal data: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

special categories of personal data: Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be personal data of special nature

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Data subject means the natural person, whose personal data is processed,

Data registry system means the registry system which the personal data is registered into through being structured according to certain criteria,

Controller means the natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system,

processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Anonymizing means rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data,

Law: Law no 6698 on the protectıon of personal data

Board means the 'supervisory authority' established by Law no 6698.

Committee means the committee responsible for implementation of this Data Protection and Processing Policy and other policies and directives adopted in order to ensure compliance with the Law.

2. PRINCIPES REGARDING PROCESSING OF PERSONAL DATA

AME adheres to the principles relating to Processing of Personal Data, as set out in the GDPR and Article 4 of the Law, which require Personal Data to be:

a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

Personal data are processed in accordance with the law and in conformity with rules of bona fides. Accordingly, the Company acts in accordance with the legislation in force in all kinds of personal data processing processes and abides by the rules of honesty.

b) Accurate and where necessary kept up to date (Accuracy);

Data controllers are responsible for setting up and implementing necessary processes to ensure that the personal data they process are accurate and up to date. In this direction, AME provides the data subjects with the opportunity to update their data and takes the necessary measures to ensure the correct transfer of the data to the databases. The data subject is responsible for the accuracy and currency of the data transmitted to us.

c) Collected only for specified, explicit and legitimate purposes (Purpose Limitation);

Data controllers are obliged to inform data subjects about the purposes of processing of their personal data in line with the notification obligations prescribed under the Law. Accordingly, AME restricts data processing activities to specific and legitimate purposes and clearly informs data subjects within the help of privacy notices regarding these purposes.

d) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimization);

Personal data are processed by AME in connection with and limited to this purpose to the extent necessary for the purpose notified to the data subject at the time of their provision.

e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

If a certain period of time is determined within the scope of the legislation in force, the data are stored for this period. If such a period is not specified in the legislation, reasonable retention periods are determined by considering the purpose of data use and Company procedures, and the data is kept limited to this period. The Company has retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. We recommend interested parties to see our Data Retention and Management Policy which is available at our web site.

3. PURPOSES FOR DATA PROCESSING

3.1. Personal data is processed by AME for the purposes listed below in accordance with the Law which allows Processing for specific purposes and principles. The company undertakes to process personal data in accordance with applicable legislation and contractual obligations. Our company will only carry out data processing activities if and to the extent that at least one of the following issues is valid:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,

(b) the Processing is necessary for the performance of a contract with the Data Subject or to take steps at the data subject's request before a contract is entered into;

(c) Processing is necessary in order to meet our legal compliance obligations.;

(d) To comply with national and international principles and regulations regarding the identification of customers, to comply with the information storage, reporting and information obligations stipulated by legislation and administrative directives,

(e) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(f) Processing is necessary for the performance of a task carried out in the public interest or for the implementation of an official duty given to our Company

(g) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

(h) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.

3.2. The personal data collected from the data subjects listed in the article 1.3. of this Policy is processed by the Company pursuant to conditions specified in the Article 5 and 6 of the Law No 6698 and within the scope of following purposes:

- Planning and Execution of Business Activities
- Market Research
- Carrying out purchasing and tender processes,
- Execution of invoice and progress payment processes,
- Managing finance and accounting procedures,
- Planning and Execution of Corporate Governance and Sustainability Activities,
- Planning Human Resources Processes,
- Planning and Execution of Corporate Relations and Communication Activities,
- Planning Information Security Processes,
- Installing and Managing Information Technology Infrastructure,
- Ensuring Security in Company Premises and / or Facilities and Service Areas
- Preparation of Personal Data Inventory
- Planning and / or Execution of Internal and External Training Activities,
- Following Legal Affairs,
- Planning and Execution of Orientation Activities inside the Company,
- In case of we participate to an organization, for registering participants,
- Planning and / or Execution of Efficiency / Productivity and / or Appropriateness Analysis of Business Activities,
- Introducing Employees, Resellers etc. in Social Media Platforms,
- Reporting within the framework of cooperation with stakeholders,
- Processing in order to ensure that Company and personal data remain correct and up to date,
- Participant Registration in Events / Trainings Organized by the Company, Arrangement of Certificates / Participation Certificates, Determination of Award / Gift Owners and Delivering awards and gifts in the name of the Company,
- Communicating with relevant parties in order to measure satisfaction levels of our services and products,
- Planning and implementing emergency response plans and protocols,

- Including those relating to subject access requests (SARs); Evaluating and Responding to All Questions, Requests, Suggestions, Complaints and Applications Transmitted to us in a Written, Verbal or Electronic form,

3.3. As part of the running of AME's commercial activities, the company obtains contact details of individuals (clients, prospects, service providers etc.). These individuals may be acting alone or as part of an organization.

3.3.1. Personal data we collect within this context are primarily email addresses, telephone numbers and postal addresses, but could also include LinkedIn information and other contact details. Our understanding is that these details may be considered to be within the scope of GDPR and Law No 6698 if, and only if they can be used to identify named individuals. For the purpose of this policy, contact details that can be identified only with organizations, or with groups etc. within organizations (for example, a company office address or group email address), are assumed to be outside the data protection legislation's scope.

3.3.2. To comply with Ministry of Finance requirements, The Company needs to obtain a postal address for each client that we work for, to be included in invoices that are issued.

3.3.3. For future reference, The Company may store this postal address in a list of client details on The Company Server if it relates to an organization, or group etc. Within an organization, but not if it is an individual's address. In either case, The Company may include it in the contacts list in an email account, if The Company thinks it may need it for potential future invoices.

3.3.4. MAs part of normal email correspondence, email addresses are automatically recorded in the email accounts that are used by AME staff. However, The Company does not store these addresses in a separate file, unless they are group email addresses that The Company may need to refer to – for example, the addresses of an accounts team that The Company should send invoices to. In these cases, The company may need to save the aforementioned e-mail addresses in a list of client's details in order to store the electronic mail addresses online in mobile phone and internet applications that store files such as files or pictures like Dropbox. When researching potential clients, service providers etc., The Company may store individuals 'company – based' email addresses in spreadsheets if, and only if, The Company has obtained them from publicly available sources (such as a company website). The Company will not do this for email addresses associated with individuals outside organizations.

3.3.5. The Company website does not have a login system for visitors. The Company does not collect email addresses via the website, other than those that are automatically added to a list when visitors contact The Company and specify their email addresses – The Company does not process this data or store it elsewhere.

3.3.6. The Company uses mailing lists to inform all parties stated in section one of information relevant to these parties. The mailing lists are held in a secure location on The Company Server and also on a secure mailing system. In order to prevent data loss on the mail server, backups are taken periodically, and these backups are stored in our cloud servers.

IP-based firewall blocks and relevant necessary security measures are taken on the server against entry attempts with incorrect password.

As part of normal business communication, individuals' telephone numbers may be stored (automatically or manually) in the contacts list on The Company's mobile phones or landline phones.

3.3.7. A number that is stored on The Company mobile telephones might be automatically synchronized into the contacts list in an email account associated with that phone. The Company might also add it to one of these contacts lists manually, if The Company thinks this will help to contact the person.

3.3.8. In order to process the above data, AME relies on legitimate interests of the company for contacting people within organizations or groups about business and related matters, and to include postal addresses in invoices. From a data Protection point of view, The Company believes these constitutes a 'lawful basis' for use of the data.

The data referred to in the above sections is stored on The Company computers that are used by AME staff members, within The Company Server. The Company computers require a password on start up. If work is undertaken off site, The Company staff members are required to enter a password to access The Company Server. The Company email accounts are password protected, and The Company mobile telephones requires a PIN code upon launching and restart.

The Company retains each postal address (at least in invoices, and sometimes also in The Company's spreadsheet of client details for ten years from the date when it was last used. After that, it will be deleted without any further delay on request from the client, or it may be deleted as part of a 'housekeeping' exercise.

If someone sends The Company an electronic document containing contact details (for example, the joining instructions for a training course), The Company will not be obliged to delete the document or redact those details, as they will have been supplied to The Company voluntarily. However, The Company will delete the document or redact the details on request from the document provider or Data Subject, unless this would prevent The Company satisfying any legal requirements.

For organizational clients, consent may be given by either (a) a primary contact in the organization, (b) another person in a suitable position of authority, or (c) the Data Subject.

3.4. Conditions for Processing of Sensitive Data;

3.4.1. Our workers who are likely to come into contact with petroleum products that contain harmful substances such as beryllium, toluene, lead and zinc due to their occupational exposure are considered to be in an occupational group that is at high risk in the context of the occupational health and safety (OHS) Regulation. As required by the ministry of family, labor and social services, AME needs to analyze the concentration of occupational exposure from individual analytical values in order to evaluate the chemicals that workers may be exposed to

in the workplace and to keep the exposure time and level within the allowable exposure limit. Accordingly, The Company carries out periodic blood and urine measurements of our workers for the purpose of implementation of exposure measurements of our workers, validation of exposure measurement results and similar exposure groups, comparison of occupational exposure limit values and results and reporting the results in accordance with modalities and principles specified in Regulation on Occupational Hygiene, Test and Analysis Laboratories and Workplace Environment - Comparison of Respiratory Chemical Substances with Limit Values and a Guidelines for Assessment of the Measurement Strategy - TS EN 689: 2018 + AC and current versions of similar standards.

3.4.1.1. AME implements aforementioned measurement activities since this processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of local law. Our main object is to protect our work force against the harmful effects of the materials and working environment conditions and to provide a safe working environment. As per Article 9(3) of the GDPR, aforementioned data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Turkish law or rules established by national competent bodies.

3.4.2. Besides from aforementioned reasons; AME does not actively collect or store 'sensitive personal data' as defined in the GDPR and personal data of special nature in Law No 6698, such as ethnic origin or religious or political beliefs. AME may only process sensitive personal data only if the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Turkish law provide that the prohibition of processing of sensitive data may not be lifted by the data subject and if one of the following applies:

a. processing relates to personal data which are manifestly made public by the data subject;

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Company or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Turkish legislation or a collective agreement pursuant to Turkish Labor law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

e. processing is necessary for reasons of substantial public interest, on the basis of Turkish legislation which shall be proportionate to the aim pursued, respect the essence of the

right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

f. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Turkish law or pursuant to contract with a health professional and subject to professional secrecy;

g. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats (e.g. epidemic and pandemic) to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Turkish law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

3.4.3. If such data is contained within a document that the Company is asked to work on:

· AME will not use or share data in any way, other than sharing the document, as necessary, with other parties involved in the project.

· AME will delete the document if requested to do so by the client or Data Subject, after the work is completed.

3.4.5. In order for your personal data to be processed for some specific purposes, we are to obtain your explicit consent pursuant to Law No. 6698. The purposes of processing and categories of data that can be processed with your explicit consent on any platform are listed below:

- Communication details of our staff members' relatives in order for us to communicate in case of an emergency;
- Information collected for travel, accommodation and transfer arrangements for purposes such as in-house trainings, activities, organizations.
- Information collected within the framework of training activities organized by the Company;
- Information collected for Staff Portal memberships,
- Information collected and recorded in the Company's ERP (Enterprise Resource Planning) systems to carry out internal transactions.

4. DATA CATEGORIES THAT WILL BE PROCESSED BY THE COMPANY

Categories of personal data that are listed below may be processes by the Company if one or more legitimate purposes specified in this Policy exist pursuant to principles and modalities specified in the Law and Article 2 of this Policy.

Personal Data Categories	Explanation
Identity Details	Identity information relating to an identified or identifiable natural person. E.g.: name-surname, T.R. identity number, identity card information, driver's license, passport, marriage certificate, certificate of identity register information, CV, signature information, tax number, social security number, vehicle plate information.
Communication Details	e.g. : phone number, e-mail information, address information, fax number, IP address.
Location Data	It refers to information that determines the position of the employees while using the vehicles that belongs to Company and given to them in order to be used within the scope of the services carried out by the Company. e.g.; GPS location, travel data, etc.
Information concerning Family Members and Relatives	Information about family members, relatives and other persons who can be reached in case of emergency, collected solely for protecting the vital interests of data subjects. E.g.; name-surname, telephone number etc. of persons such as spouse-parent-child etc.
CCTV Footage and other security data	It refers to all kinds of information regarding the entrance and exit details relating to an identified or identifiable natural person in physical areas that are the property of the Company or where our Company provides services. E.g. ; Entry and exit log records, visitor records, CCTV footage, fingerprint records and records taken at the security point etc.
Risk Management Data	Personal data processed via methods used in accordance with the generally accepted legal rules, commercial custom and principle of bona fide for the purposes of managing commercial, technical and administrative risks.
Corporate Data	All kinds of personal data obtained and maintained within the

	corporate structure of the company For example: authorized signatory list, company manager and employee information, title information, position information, etc.
Financial Data	It refers to any kind of information that is obtained according to the nature of the legal relationship between the person and our Company and serves to finance this relationship or shows the financial result of this relationship. E.g.; bank name, bank account number, tax identification number, IBAN number, credit card information, assets data, income information, financial risk report etc.
Legal Affairs and Regulatory Compliance Data	The personal data processed within the scope of the determination, follow-up and collection of the commercial payables and rights of the company and compliance with the legal obligations and Company policies and the data included in the documents such as court and administrative authority decisions.
Transaction Security Data	Information that serves to show that relevant data subject is authorized to make transaction and link the individual to relevant transaction such as online financial payment or order details.
Visual/Audio Data	All kinds of photo and camera recordings, sound recordings etc. relating to an identified or identifiable natural person excluding the records acquired within the scope of security camera footage.
Documentary Records	It refers to information relating to an identified or identifiable natural person registered on documents signed with our companies. E.g. contracts, contract termination notices, additional protocols, notices and summons issued by judicial and administrative authorities, etc.
Audit and Supervision Related Data	Audit and inspection and disciplinary proceedings reports, related interview records and similar records.
Employee's Personal	Data relating to personal benefits and other social security data relating to an identified or identifiable natural person

Information	processed according to an employment contract signed with the Company. Payroll information, bank receipts, payroll records, data required by social security institutions, fringe benefits, annual leave-excuse reports, shift change forms, declaration and consent approval documents, employment contracts, declarations and undertakings given for information security, performance evaluation reports and, all mandatory information that must be entered into personnel file.
Prospective Employee Data	It refers to all kinds of information obtained for the establishment of the employment contract with a prospective employee. E.g.; CV information, interview notes, Turkish ID number, retirement information, address, telephone, e-mail, personality inventory records, data obtained from institutions and portals that provide recruitment services.
Sensitive Personal Data	Pursuant to Article 6 of the Law No 6698; personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data and public security data obtained due to the execution of the operating agreements even if concluded with private law real and legal persons.
Request/Complaint Management Data	All kinds of requests and complaints brought to attention of the Company and all kinds of reports regarding their receipt and evaluation of them constitute request / complaint management information, if they are related to an identified or identifiable natural person.
Reputation Management Data	Personal data relating to an identified or identifiable natural person that are collected for the purpose of protecting the commercial reputation of the Company (E.G.; comments done regarding the Company)

5. DATA TRANSFERS

5.1.General Conditions for Data Transfers

Article 8 of the Law No 6698 makes a distinction between transfer of personal data inside Turkey and abroad.

As per the aforementioned provision personal data can only be transferred to third parties if one of the Conditions listed below applies:

· the data subject has given explicit consent,

· processing is explicitly prescribed by law,

· processing is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid.

· processing of personal data is necessary to honor contractual obligations emanating from a contract signed with the data subject, provided that it is directly related to the conclusion or fulfilment of that contract.

· processing is mandatory for the controller to be able to perform his legal obligations,

· processing relates to personal data which are manifestly made public by the data subject;

· processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity,

· processing is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject,

Sensitive personal data can only be transferred under specific Conditions provided that sufficient measures are taken pursuant to paragraph 2 of the aforementioned Article. Accordingly, the Company may transfer sensitive personal data under circumstances described below:

· Personal data, excluding those relating to health and sexual life, listed in the first paragraph may be processed without seeking explicit consent of the data subject, in the cases provided for by laws,

· Personal data relating to health and sexual life may only be transferred, without seeking explicit consent of the data subject, by any person or authorized public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

Your personal data may be transferred for the purposes mentioned above to following parties in accordance with data processing conditions and modalities prescribed by Article 8 and 9 of the Law No 6698: domestic governmental institutions and organizations, law

enforcement agencies, courts and enforcement offices, business partners, service provider companies and their officials, third party real and legal persons with whom we are in contact, banks, our group companies and affiliates, our suppliers and support service providers.

5.2. Transfer of personal data abroad

The Company may transfer the personal data it processes by taking the necessary security measures to third parties registered abroad and to the company headquarters located in the State of Kansas (645 E. Douglas, Suite 100, Wichita, KS 67202, USA) and our affiliates in Europe.

The Company may transfer personal data abroad under circumstances described below:

· the data subject has given explicit consent or;

· Personal data may be transferred abroad without explicit consent of the data subject provided that one of the conditions set forth in the second paragraph of Article 5 and the third paragraph of Article 6 of the Law No 6698 exist and that;

· sufficient protection is provided in the foreign country where the data is to be transferred and;

· The Company signs a data processing agreement with the data controller established in a foreign country in order to guarantee a sufficient protection in writing and the Board has authorized such transfer, where sufficient protection is not provided.

5.3.To whom your personal data will be transferred?

AME may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions. In order to comply with our obligation as a data controller to inform data subjects as prescribed by the Article 10 of the Law No 6698, we hereby provide details about the recipients to whom we may transfer personal data and purposes for which we process personal data:

Groups of real and legal persons to whom we may transfer personal data	**Explanations regarding recipients of personal data**	**Purpose of Data Transfer**
Business Partner	The parties with whom the Company conducts commercial activities, regardless of their	Personal data can be transferred in order to ensure the fulfillment of the objectives of the business

	nominations.	partnership established for the purposes of carrying out various projects and receiving services in the course of Company's commercial activities.
Group Companies	All companies and subsidiaries that constitute the group	Limited to purposes such as planning the company's commercial activities and continuing its activities and audit
Supplier	Third parties that provide services to our Company in any way based on the service agreement signed within the scope of the commercial activities of our company.	Pursuant to instructions given by the Company and based on the contract between the supplier and the Company, limited data transfers may be done to the parties that provide services for the continuation of the commercial activities of the Company.
Shareholders	Real persons who hold Company's shares	Within the scope of company law and corporate communication processes of the company, necessary personal data will be transferred in accordance with the provisions of the relevant legislation and only limited to these process activities.
Company Senior Officers	Members of the company's board of directors and other real persons who are assigned as authorized signatories of the Company.	Personal data will be transferred for the purposes of determining the business strategies of our company, ensuring the senior management and making the necessary audits in accordance with the provisions of the relevant legislation and only limited to these purposes.

Legally Authorized Public Institutions and Organizations and Private Law Persons	Public institutions and organizations and private law entities authorized to request information and documents from the Company in accordance with the provisions of the relevant legislation	Personal data will be transferred to relevant public institutions and organizations and private organizations within the framework of the legal authority granted to them pursuant to provisions of relevant legislation and only for the purpose they require.

6. WHAT RIGHTS DATA SUBJECTS HAVE CONCERNING THEIR DATA?

Data subjects can exercise their rights in respect of their personal data by sending their requests regarding the rights granted to them in accordance with Article 11 of the Law in writing or by other means to be determined by the Board. In the event of a request submitted by a third party on behalf of the data subject, a power of attorney certified by a notary public on behalf of the applicant must be attached to the request. The Company has established corporate procedures in order to provide a framework for responding to subject access requests (SARs). It is our policy to ensure that requests by data subjects covered by these procedures to exercise their rights in respect of their personal data are handled in accordance with applicable law. As stipulated in Article 13 of the Law, the Company will conclude SARs by giving a written reply free of charge within thirty days at the latest, depending on the nature of the request. However, in case the response requires an additional cost, the Company reserves the right to demand the fee in the tariff determined by the Board of Directors.

6.1. The Company acknowledges and respects the rights afforded to Data Subjects under the Article 11 of the Law including following rights:

- to learn whether his/her personal data are processed or not,
- to request information if his personal data are processed by the The Company,
- to learn the purpose of his/her data processing and whether this data is used for intended purposes,
- to know the third parties to whom his/her personal data is transferred at home or abroad,
- to request the rectification of the incomplete or inaccurate data, if any,
- to request the erasure or destruction of his personal data under the conditions laid down in law,
- to request notification of rectification, erasure or destruction operations carried out pursuant his/her request to third parties to whom his personal data has been transferred,
- to object to the processing, exclusively by automatic means, of his/her personal data, which leads to an unfavorable consequence for the data subject,
- to request compensation for the damage arising from the unlawful processing of his/her personal data.

The Company may accept applications submitted by SARs in accordance with Article 11 of the Law or reject them stating the precise reasons for the refusal.

- Right to complain to the Board about any alleged misuse of data

If the application is declined, the response is found unsatisfactory or the response is not given in due time, the data subject may lodge a complaint with the Board within thirty days of receipt of the response of the Company, or within sixty days as of the application date, in any case.

6.2.How data subjects can exercise their rights in respect of their personal data?

Data subjects can fill the Data Subject Application Form whose link can be found in our web site in order to exercise their rights in respect of their personal data. Applications must be send with documents that s-establish the identity of the data subject using one of the following modalities:

· By filling the aforementioned form and delivering the wet signed copy by hand, via notary public or by registered mail to the following address "Karum İş Merkezi İran Caddesi No: 21/394 Kavaklıdere Çankaya / Ankara",

· By filling the aforementioned form and attaching a secure signature in accordance with the provisions of Law No 5070 on Electronic Signatures and e-mailing to "kvkk@ame.com.tr",

The company reserves the right to request information from the applicant in order to verify the identity of the data subject and direct questions to data subject in order to clarify the matters specified in the application.

6.3.Exceptions that are not subject to Law No 6698

Article 28 of the Law No 6698 restricts the scope of the obligations and rights provided in the following cases where:

a) personal data is processed by natural persons within the scope of purely personal activities of the data subject or of family members living together with him in the same dwelling provided that it is not to be disclosed to third parties and the obligations about data security is to be complied with.

b) personal data is processed for the purpose of official statistics and for research, planning and statistical purposes after having been anonymized.

(c) personal data is processed with artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defence, national security, public security, public order, economic security, right to privacy or personal rights are not violated or they are processed so as not to constitute a crime.

(d) personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned to maintain national defence, national security, public security, public order or economic security.

(e) personal data is processed by judicial authorities or execution authorities with regard to investigation, prosecution, criminal proceedings or execution proceedings.

Pursuant to Article 28/2 of the Law No 6698, data controller's obligation to inform, the rights of the data subject, excluding the right to demand compensation, and requirement of enrolling in the Registry of Data Controllers shall not be applied in the following cases where personal data processing:

a) is required for the prevention of a crime or crime investigation.

b) is carried out on the data which is made public by the data subject himself.

c) is mandatory for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public institutions and organizations and by professional associations having the status of public institution, assigned and authorized for such actions, in accordance with the power conferred on them by the law,

d) is mandatory for protection of State's economic and financial interests with regard to budgetary, tax-related and financial issues.

7. MEASURES TAKEN BY THE COMPANY TO PROTECT PERSONAL DATA

AME considers that necessary technical and administrative measures should be taken in order to protect the rights and freedoms of natural persons with respect to processing personal data. In this context, the Company will determine its policies regarding its internal operation and take the necessary measures to meet the principles of data protection from the beginning and privacy by design. AME aims to implement appropriate technical and organizational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the Law and protect the rights of data subjects while taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing both at the time of the determination of the means for processing and at the time of the processing itself. The Company shall take measures described below to the extent necessary in order to ensure security of personal data:

7.1.Determination of Risks and Threats to Personal Data

In order to ensure the security of personal data, the Company firstly determines what personal data it holds by creating an inventory in order to accurately determine the probability of possible risks that may arise in relation to their protection and the losses that may occur and takes the relevant measures. Following criteria is used to determine risks:

i. Whether personal data we hold contains any sensitive data,

ii. The degree of confidentiality required by the natüre of personal data processed,

iii. In case of data security breach, the nature and quantity of the damage that may occur for the person concerned is taken into account.

7.2. Determination of Personal Data Security Policies and Procedures: We establish policies and code of conduct for the management of risks and security breaches that may occur for data categories determined on the basis of personal data inventory. The Company aims to update these policies and procedures regularly to ensure continuous compliance and security.

7.3. Measures taken in respect of data security: AME implements measure to limit the purpose of data processing activities by ensuring that personal data are collected for explicit and legitimate purposes specified in this Policy and that they are not processed in a way that is not suitable for these purposes and we do not keep the data for longer than necessary. In this context, the Company regularly evaluates the need for processing personal data and whether the data is stored in the right place. In addition, personal data, which are not required to be accessed frequently and kept for archival purposes, despite being suitable for the purpose for which they are processed, are kept in a more secure environment in order to prevent unauthorized access.

AME takes reasonable technical and administrative measures to prevent unauthorized access, accidental data loss, deliberate deletion or damage of data in order to ensure the security of personal data which are summarized below:

7.3.1. Technical Measures:

Technical measures implemented by the Company in order to prevent illegal Access to personal data are listed below:

- Pseudonymisation is used if necessary for data security,
- If required for data security, the relevant person data is anonymized,
- Reasonable cyber security measures are taken and implemented, periodically controlled and updated.
- Technical measures taking into account the state of the art and risks are implemented and measures taken are periodically updated and amended if necessary.
- Access control and account authorization solutions are implemented in accordance with the requirements determined on the basis of need to know principle.
- The technical measures taken are periodically reported to the relevant person in accordance with the internal audit mechanism, the issues that pose a risk are re-evaluated and the necessary technological solution is applied.
- Software and hardware, including virus protection systems and firewalls, have been installed.
- Access to personal data is registered in log books.
- We ensure data security by using software and hardware containing virus protection systems and firewalls and gateways,
- Almost all software and hardware are installed and configured. In addition, it is ensured that the security gaps are documented, especially the old version software and services are kept up-to-date, instead of being removed from the device and deleted.

- If personal data is to be obtained from different websites and / or mobile application channels, connections are made via SSL or a more secure channels.

7.3.2. Administrative Measures

Administrative measures implemented by the Company in order to prevent illegal access to personal data are listed below

- Personal data processing activities are tracked on a business unit basis,
- Necessary inspections are made in order to ensure the implementation of the provisions of the Law in accordance,
- Continued compliance of data processing activities with the Law is ensured via internal policies and procedures,
- Our employees are required to sign non-disclosure and confidentiality declaration specifying that they cannot disclose the personal data they have processed in the course of their duties to third parties in violation of the provisions of the law and that they cannot use them for purposes other than purpose of the processing and that this obligation shall continue even after they leave their duties, and in this direction, aforementioned obligations constitute a part of our employees' labor contract.
- Access authorizations are granted in accordance with the nature of the data accessed within the company,
- Access to sensitive personal data are subject to more stringent conditions,
- Systems used inside the Company can only be accessed using a username and password,
- When creating passwords and codes, it is mandatory that combinations consisting of uppercase and lowercase letters, numbers and symbols are preferred instead of numbers or letter strings that are associated with personal information and are easy to guess,
- The Company implements corporate access control policies and procedures which establish an access authorization and control matrix for data owners.
- The number of password entry attempts is limited,
- Passwords and Access codes are changed at regular intervals,
- Administrator account and admin authority are granted only when needed,
- Accounts and Access rights of employees no longer work for the Company are annulled without delay,
- Antivirus and antispam products are used that regularly scan the information system network and detect dangers,
- We only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place through data processing agreements which contain specific obligations and penalties for data exporter and data recipient.
- Necessary administrative measures are taken and awareness programs are carried out to inform all employees, especially those who are authorized to access personal data, about their duties and responsibilities in the field of data privacy.

7.4.Data Protection Impact Assessment(DPIA)

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Company is required to, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

A DPIA will be carried out when implementing major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) Automated Processing including profiling and automatic decision making;

(c) large scale Processing of Sensitive Data; and

(d) large scale, systematic monitoring of a publicly accessible area.

We will seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

7.5. Notification of a personal data breaches to the supervisory authority and data subjects

1. If we discover that there has been a breach of personal data that poses a risk to data subjects' rights and freedoms, we will report this to the Board within 72 hours of discovery. We will also record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to data subjects' rights and freedoms, AME will inform relevant parties of the breach and provide them with information about its likely consequences and the mitigation measures we have taken.

2. The Company will not be required to inform individuals as it is described in the above paragraph 1 about the personal data breach where:

(a) The Company has implemented appropriate technical and organizational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorized to access it, such as encryption.

(b) The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialize.

(c) It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to inform all affected individuals.

8. Data Retention Period

AME stores Personal Data for the period specified in this legislation, as required by law. If a period of time is not regulated in the legislation regarding how long personal data should be stored, Personal Data is processed for a period that requires processing in accordance with the Company's processes and manuals and best practices accepted in the field of activity, depending on the activity carried out while processing that data. When Personal Data is no longer needed for specified purposes, it is deleted or anonymized in accordance with the Group's data retention policy, as set out in the Data Retention and Management Policy.

If the retention periods determined by the relevant legislation and purpose of processing personal data has ended, personal data can only be stored in order to provide evidence in possible legal disputes or to assert the relevant right related to personal data or to establish a defense. In the establishment of the periods here, taking into account the period of limitations for relevant data category, the retention periods are determined based on the previous requests submitted to the Company on the same issues before. In this case, the stored personal data are not accessed for any other purpose, other than it is required to be used in the relevant legal dispute. Here, too, after the mentioned period expires, personal data are deleted, destroyed or anonymized.

9. Erasure, Destruction or Anonymization of Personal Data

Company staff and representatives including representatives with whom our company or our company cooperates or authorize to act on our behalf, retain the personal data that have been processed according to law for the period required by the purposes of processing stipulated in the Article 138 Turkish Penal Code, Article 7 of the Law no 6698 and provisions of relevant legislation and specified in this Policy.

Without prejudice to the provisions of specific laws regarding the deletion, destruction or anonymization of Personal Data, the Company deletes, destroys or anonymizes the Personal Data ex officio or upon the request of the data subject, when Personal Data is no longer needed for specified purposes.

While deleting personal data, these data are destroyed in a way that they cannot be used and retrieved in any way. Accordingly, Personal Data is irreversibly deleted from medias they have been stored such as documents, files, CDs, floppy disks, hard disks. Destruction of Personal Data, on the other hand, refers to the destruction of materials suitable for data storage such as documents, files, CDs, floppy disks, hard disks in which the data are recorded so that the information cannot be recovered and used. Anonymization of personal data refers to rendering the personal data no longer be attributed to a natural person by the use of additional information.

10. Administrative Division of Roles inside the Company for Data Protection Issues

"Personal Data Protection Committee" has been established within AME to implement this policy and other related policies related to this policy. The Committee is responsible for carrying out the actions determined by the senior management for compliance. constitution and responsibilities of the Committee is shown below.

Nº	ASSIGNED POSITION	FUNCTION	NAME SURNAME
1	HEADQUARTERS	General Director	Baran Erdem KAYA
2	HEADQUARTERS	COO	Halil AKTAŞ
3	HEADQUARTERS	Assistant General Manager	Çağatay BEYDOĞAN
4	HEADQUARTERS	Human Resources Manager	Derya ERBAŞ
5	HEADQUARTERS	Assistant to Human Resources Manager	Can DENİZ

In this context, the following minimum actions will be taken by the Committee:

- To determine the relevant policies regarding the processing and protection of personal data and the measures to be taken in order to comply with the legislation,
- Submit aforementioned policies and actions for the approval of the Senior Management; supervise their implementation and coordination,
- To determine the modalities of how the policies regarding the processing and protection of personal data will be implemented and how the audits will be carried out, to make necessary assignments after receiving the approval of the senior management,
- To determine the risks that may occur in the personal data processing activities of the company and to ensure that necessary measures are taken; submit suggestions for risk improvement to the approval of senior management,
- To ensure that staff are adequately trained in order to support the implementation of data protection laws and Company policies in this field,
- To decide on how to response to data subjects' request at the highest level,
- To make necessary arrangements within the company in order for the company to fulfill its obligations with respect to data protection,
- To ensure communication and cooperation with the Board and other institutions.

11. (CCTV) USAGE

Visual and audio data of visitors and staff processed via closed circuit camera system located at headquarters of AME, in other physical areas where service is provided, for purposes such as preventing criminal behavior in the building, ensuring the safety of the building, its surroundings, tools and equipment, visitors and employees, and contractual obligations can be obtained and stored only for the period required for these purposes. The Company implements necessary administrative and technical measures to ensure the security of personal data obtained by CCTV cameras.

Aforementioned data is processed if it is compulsory to fulfill its legal obligations such as it is stipulated by law pursuant to article 5/2 / a of Law No 6698, it is mandatory for the Company to be able to perform our legal obligations such as supervision and protection of employees, data processing is mandatory for the establishment, exercise or protection of any right as per Article 5/2(e) and it is mandatory for the legitimate interests of the Company provided that this processing shall not violate the fundamental rights and freedoms of the data subject as per Article 5/2(f)

12. WEBSITE AND COOKIE POLICY:

On the websites owned and managed by the company, the internet movements of the visitors within the site are recorded by technical means (such as "cookies") to analyze user activity in order to improve the website. Pursuant to provisions of Law No 5651 on Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication, IP address or IP address of your proxy server and the domain name requested, the date and time of the website visit, when our corporate website is visited by users due to the fact that we are the hosting provider.

We do not use analytical cookies, targeting and advertising cookies on our corporate website, and only mandatory cookies are used for our website to function correctly. Users can opt out of using cookies on websites owned and managed by the company, change their types or functions, or add new cookies.

AME will process the personal data obtained through the cookies in accordance with the Law no 6698 and the terms and conditions of this Policy. Detailed explanations on the protection and processing of personal data in terms of corporate website can be found in the "Privacy Policy" section.

POLICY UPDATES AND AMENDMENTS:

This policy will be reviewed at regular intervals, and if necessary, it may be amended to reflect changes in our operational activities, to comply with best practices in data management, security and data control and new legislative provisions. In case of changes, necessary announcements will be posted on our website, and we recommend relevant parties to visit our website regularly to be aware of these changes.