Data Retention and Management Policy

IGDP_P3 VERSION 1.00

ALADDIN MIDDLE EAST LIMITED – TURKEY BRANCH OFFICE

Data Retention and Management Policy

Purpose:

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 Retention and Management Policy and aims to provide information relating to modalities of how we retain and delete personal data pursuant to Law No 6698 on Personal Data Protection (hereinafter referred as "Law").

AME's corporate policy is to ensure that company employees, employee candidates, service providers, visitors and other third parties' personal data are processed according to the basic principles stated in the Personal Data Protection and Processing Policy, the Turkish Constitution, international agreements, Law, secondary legislation and other relevant legislation and relevant individuals can exercise their rights effectively with respect to their personal data.

The protection of personal data and the observance of the fundamental rights and freedoms of individuals whose personal data are processed are the basic principles of our policy regarding the processing of personal data.

The Company carries out its activities and transactions regarding the storage and destruction of personal data in accordance with the Policy prepared in line with the aforementioned principles.

Scope:

Personal data of Company employees, employee candidates, suppliers, customers, visitors and other third parties are within the scope of this Policy and the provisions of this Policy will be applied in all recording environments where personal data is processed by the Company or managed by the Company, and personal data processing activities we implement.

This Policy covers all personal data subject to data processing activities of our Company pursuant to the Law. In addition, unless otherwise stated in this Policy, the documents referred include both printed and electronic copies.

Abbreviations and Definitions:

Recipient	A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
Explicit Consent	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,
Anonymization	Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data
Company Staff	Individuals who work for the Company pursuant to a labor contract
EDMS	Electronic Document Management System
Service Provider	A natural or legal person providing services under a specific contract signed with the Company.
Record Medium	Any medium containing personal data that is fully or partially automated or processed in non-automatic ways provided that it is part of any data recording system
Data Subject	the natural person, whose personal data is processed,
Filing System	Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
Authorized User	Except for the person or unit responsible for the technical storage, protection and backup of data; Individuals who process personal data within the organization of the data controller or in line with the authority and instruction received from the data controller,
Pseudonymisation	Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Disposal	Deletion, destruction or anonymization of personal data.
Electronic Medium	Media in which personal data can be created, read, changed and written with electronic devices,
Non-electronic Medium	All written, printed, visual, etc. other mediums other than electronic media,
Law	Law No 6698 on Personal Data Protection,
Personal Data	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.
Data Processing Inventory	An inventory that details personal data processing activities carried out by data controllers depending on the business processes; the purpose of processing personal data and the legal reason, the data categories, the transmitted recipient group and the data subject group, and that explains the maximum retention period required for the purposes for which the personal data is processed, the personal data foreseen to be transferred to foreign countries and the measures taken regarding data security
Processing	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,
Board	Supervisory authority' established by Law no 6698,
Sensitive Data/ personal data of special nature	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
Periodic Destruction	The deletion, destruction or anonymization process to be carried out ex officio at repetitive intervals specified in the personal data storage and destruction policy in case all the conditions for the processing of personal data in the law no longer apply.
Policy	Data Retention and Management Policy,
Data processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Data Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data,
Registry of Data Controllers (VERBİS)	The information system that data controllers must use in the application to the Registry and in other related transactions related to the Registry, accessible on the internet, created and managed by the Presidency of the Board.
Regulation	Regulation on Deletion, Destruction or Anonymization of Personal Data.

RECORD MEDIUMS COVERED BY THIS POLICY

AME stores all personal data subject to data processing activities within the scope of the Law, in the mediums specified below, where personal data are processed completely or partially automatically or by non-automatic means provided that it is a part of any data recording system.

Electronic Media	Non-electronic Media
✓ Servers (Domain, backup systems, e-mail, database, web, file sharing, Enterprise Application Software etc.) ✓ Software (Office applications, portal, EDMS, VERBİS) ✓ Information security devices (firewall, intrusion detection and blocking, log file, anti-virus, etc.) ✓ Personal Computers (Desktop, Laptop) ✓ Mobile devices (telephone, tablets etc.) ✓ Optic disks (CD, DVD etc.) ✓ Removable disks (USB, Memory Cart etc.) ✓ Printer, Scanner, Photocopy Machines ✓ CCTV Footage ✓ Web Page and portal	✓ Paper ✓ Manual Filing systems (survey forms, visitor log book, disciplinary decision book, annual leave book, accounting book(ledger), occupational health book, incoming-outgoing document registry book, etc.) ✓ Written, printed, visual media

ACCEPTABLE LEGAL AND TECHNICAL REASONS FOR DATA RETENTION AND ERASURE

The Company gathers and process personal data of its staff, employee candidates, service providers, customers, visitors and other third parties according to modalities specified in this Data Processing and Protection Policy and in line with purposes outlined in Articles 5 and 6 of the Law. AME does not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements. Personal Data is deleted ex officio or at the request of data subjects 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.

EXPLANATIONS CONCERNING DATA RETENTION MODALITIES:

The processing of personal data is defined in Article 3 of the Law, it is stated in Article 4 that the Personal Data must be adequate, relevant and limited to what is necessary in

relation to the purposes for which it is Processed and should be kept for the period stipulated in the relevant legislation or for the purpose for which they are processed, and in Articles 5 and 6, the conditions for processing are outlined.

Personal data that needs to be processed within the framework of our company's activities are stored for the period stipulated in the relevant legislation or in accordance with AME's applicable records retention schedules and policies.

LEGAL REASONS FOR DATA STORAGE

Personal data processed within the framework of the company's activities are stored for a limited period of time stipulated in the relevant legislation. In this context, personal data are stored for the retention periods stipulated in the framework of relevant laws and other secondary regulations in force listed below:

- Law No. 6698 on Protection of Personal Data
- Turkish Code of Obligations,
- Public Procurement Law No. 4734,
- Social security and general health insurance law (Law No. 5510)
- Law No. 5651 on Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication
- Law No. 5018 on public finance management and control
- Law No. 213 Taw Procedure Law,
- Law No. 6331 on Occupational Health and Safety,
- Law No. 4982 on Right to Information,
- Law No.3071 on the Exercise of the Right to Petition
- Labor Code-Law No. 4857,
- Law No. 6481 on Turkish Petroleum,
- Regulation on Health and Security Measures on Work Facilities,
- Regulation on Archive Services

Personal Data is deleted after a reasonable time for the purposes for which it was being held if there is no legal provision.

REASONS FOR DATA DISPOSAL

Personal data will be deleted, destructed or anonymized without undue delay if one of the conditions set out below applies:

- Amendment or abolition of the relevant legislation provisions that form the basis of processing,
- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data were processed and there is no other legal basis for the processing;

- the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defense of legal claims;
- In accordance with Article 11 of the Law, the application requesting the deletion and destruction of personal data within the framework of the rights of the person concerned is admitted by the Board.
- the personal data has to be erased for compliance with a legal obligation to which we are subject;
- If the application of data subject is declined, the response is found unsatisfactory or the response is not given in due time, the data subject files a complaint with the Board and Board accepts the application.
- The maximum period for the storage of personal data has terminated and there are no conditions to justify the storage of personal data for a longer period.

TECHNICAL AND ORGANIZATIONAL MEASURES

AME implements reasonable and appropriate technical and organizational security measures against unlawful or unauthorized Processing of Personal Data and against the accidental loss of, or damage to, Personal Data pursuant to Article 12 and Article 6(4) of the Law and Board Resolution No. 2018/10 of 31.01.2018 with respect to sensitive data.

Technical Measures

Technical measures we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction are listed below:

- With the help of penetration tests, the risks, threats, vulnerabilities and gaps, if any, found in the information systems are determined by the Company and necessary measures are taken.
- As a result of real-time analysis and information security event management, risks and threats that will affect the continuity of information systems are constantly monitored.
- Access to information systems and authorization of users are done through access and authorization matrix and security policies for the corporate active directory.
- Necessary measures are taken for the physical security of Company’s information systems equipment, software and data.
- In order to ensure the security of information systems against environmental threats, hardware (access control system that allows only authorized personnel to enter the system room, 24/7 monitoring system, physical security of edge switches that make up the local area network, fire extinguishing system, air conditioning system, etc.) and

software (firewalls, attack prevention systems, network access control, systems that prevent malicious software, etc.) are implemented.

- Risks are identified in order to prevent unlawful processing of personal data, technical measures are taken in accordance with these risks and technical controls are carried out for the measures taken.
- Reporting and analysis regarding access to personal data are carried out by established access control procedures within the Company.
- Access to data storage areas is recorded and inappropriate access or access attempts are supervised.
- The Company takes the necessary measures to ensure that the deleted personal data cannot be accessed and reused for the relevant users.
- In case personal data is illegally obtained by unauthorized parties, a suitable system and infrastructure has been established by the Company in order to notify the relevant data subjects and the Board.
- Security vulnerabilities are analyzed and appropriate security patches are installed and information systems are kept up-to-date.
- Strong passwords requirements are implemented to access electronic media that contains personal data.
- Secure record keeping (logging) systems are used in electronic media where personal data are processed.
- We use data backup programs that ensure the safe storage of personal data.
- Access to personal data stored in electronic or non-electronic media is restricted according to access principles.
- Trainings regarding sensitive personal data have been provided for employees involved in sensitive personal data processing processes, confidentiality agreements have been signed, and the authorities of users with access to data have been defined.
- All records are logged in electronic media where sensitive data are processed, stored and / or accessed, security updates of these media are constantly monitored, necessary security tests are regularly performed and test results are recorded.
- Adequate security measures are taken in physical environments where personal data of special nature are processed, stored and / or accessed, and unauthorized entry and exit are prevented by ensuring physical security.
- When it is necessary to transfer sensitive personal data via e-mail, it is transferred encrypted using a corporate e-mail address or a Registered Electronic Mail account. When it is required to be transferred via portable memory, CD, DVD, etc., it is encrypted with cryptographic methods and the cryptographic key is kept in a different environment. When it is necessary to transfer data between servers in different physical environments, data transfer is performed between servers by setting up a VPN or using the sFTP method. Necessary precautions are taken against risks such as theft, loss or unauthorized access when data is required to be transferred via paper media and the document is sent in "confidential" format.

Organizational Measures

Organizational measures we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction are listed below:

- In order to improve the quality of employees, trainings are provided on the prevention of unlawful processing of personal data, prevention of unlawful access to personal data, protection of personal data, communication techniques, technical knowledge skills, Law No.6698 and other relevant legislation.
- Staff members' access to stored personal data is limited to the employees who have to access them as per job requirements. In determining access privileges, whether the data can be regarded as sensitive data and its importance for the Company and data subjects are taken into account. Necessary security measures are taken for entering and exiting physical environments where personal data are stored.
- Physical environments in which personal data are processed are secured against external risks (fire, flood, etc.).
- Confidentiality and non-disclosure agreements regarding the activities carried out on behalf of the Company are signed with staff members.
- Access privileges of employees whose work station has been changed or whose labor contract has been terminated are annulled without delay.
- A disciplinary procedure has been established for employees who do not comply with the Company security policies and procedures.
- Data Processing Inventory has been established according to Law.
- Data security measures are required from service providers and other stakeholders via data processing addendums and specific provisions.
- Affirmative covenants regarding confidentiality is required for relevant stakeholders.
- Periodic and random audits are conducted within the company. Confidentiality and security weaknesses that arise as a result of the inspections are immediately reported for update.
- Information security awareness trainings are offered to staff members.
- Personal Data policies are updated in December of each calendar year, risk analyzes and risk improvement studies are carried out.

PRINCIPALS REGARDING ERASURE, DESTRUCTION, PSEUDONYMIZATION OR ANONYMIZATION OF PERSONAL DATA

As per Articles 12 and 13 of the Law, AME fulfills its obligations regarding the deletion, destruction or anonymization of personal data, either ex officio or at the request of the person concerned.

In the deletion, destruction or anonymization of personal data, the company acts in accordance with the general principles set out in its policies regarding the protection and processing of personal data, technical and administrative measures, relevant legislation provisions, Board decisions and personal data storage and management policy.

All measures taken by the Company regarding the deletion, destruction and anonymization of personal data are recorded which are kept for at least two years, excluding other legal obligations.

Unless a contrary decision is taken by the Board, the Company selects the appropriate method of deleting, destroying or anonymizing personal data. Upon the request of the data subject, the Company chooses the appropriate method by explaining the reason.

Deletion of Personal Data

Deletion of personal data is the process of making personal data inaccessible and unavailable in any way for the relevant users. The Company takes all necessary technical and administrative measures to ensure that the deleted personal data are inaccessible and unavailable for the relevant users.

The Company chooses one of the appropriate methods given below for deletion, depending on the medium in which the data is recorded:

- Giving a delete command
- Dimming
- Removing the relevant user's access right on the directory where the file is located
- Deleting via software
- Deleting with database command

Destruction of Personal Data

The destruction of personal data is the process of making personal data impossible to access, retrieve and reuse in any way. The company takes all necessary technical and administrative measures regarding the destruction of personal data.

ELECTRONIC MEDIA	NON-ELECTRONIC MEDIA
For personal data that no longer needs to be stored on the servers, the system administrator will remove the access authority of the relevant users and delete them	Except for the department manager responsible for document archiving, personal data that no longer needs to be kept in a physical environment are rendered inaccessible and unusable in any way. In addition, the blackout process is also applied by drawing / painting / wiping in order to make documents illegible.
Personal data that no longer needs to be stored in electronic environment are made inaccessible and unavailable in any way for other employees (relevant users), except for the database manager.	Personal data that no longer needs to be stored in the paper environment, are irreversibly destroyed in the paper trimming machines.
Personal data that no longer needs to be stored in flash memory devices are stored in secure environments with encryption keys, encrypted by the system administrator and the access authority is given only to the system administrator.	The decision for composition of a Destruction Commission is submitted to the general manager. The Destruction Commission consists of the relevant deputy general manager, unit manager and department chiefs.

Physical destruction of the personal data stored in optical media and magnetic media is ensured via melting, burning or pulverizing. Furthermore, magnetic media is passed through a special device and exposed to a high magnetic field, making the data on it unreadable.	Destruction lists are prepared. Destruction approval is obtained from the general manager. Documents to be destroyed are made unreadable and delivered to the recycling facility in a controlled manner. Destruction procedures are also registered in electronic forms. Documentation of destruction procedures are kept.

AME chooses one of the appropriate methods, depending on the medium in which the data is recorded:

- Physical destruction
- Overtyping
- Destruction with paper shredder
- Destroying all copies of encryption keys

Pseudonymisation and Anonymization of Personal Data

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual. In order for personal data to be anonymized; personal data must be no longer be attributed to a specific data subject even through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as recycling by the data controller, recipient or recipient groups and matching the data with other data. The company takes all necessary technical and administrative measures regarding the anonymization of personal data.

AUTHORIZED OFFOCERS FOR ERASURE, DESTRUCTION, PSEUDONYMIZATION OR ANONYMIZATION OF PERSONAL DATA

Persons involved in the processes of storing and destroying personal data are trained by our company on the legislation on the Protection of Personal Data and the processing of personal data in accordance with the law. In this context, Company staff members and authorized third parties who need to access personal data due to their duties are required to store and destroy such information in accordance with the provisions of the Law and other relevant legislation. This obligation continues after termination of employment and contracts.

All units and employees of the Company, the responsible departments of the policy, are required to actively support the responsible units in taking technical and administrative measures to ensure data security in all environments where personal data are processed in order to ensure legal compliance, the appropriate implementation of the technical and administrative measures taken within the scope of the Policy, the training and awareness of the employees, their monitoring and

continuous supervision, preventing the illegal processing of personal data, preventing the illegal access to personal data.

The process of deletion, destruction or anonymization of personal data whose retention periods have expired is carried out by the relevant department authorized person of the Company.

In this context, functions and titles of the authorized officers involved in the storage and disposal processes of our Company are explained below.

TITLE	WORK STATION	FUNCTION
Director f Legal Affairs	Legal	Managing the personal data destruction process in accordance with the periodic destruction schedules and ensuring the compliance of his/her unit with data retention and management procedures.
Director of Human Resources	Human Resources	Managing the personal data destruction process in accordance with the periodic destruction schedules and ensuring the compliance of his/her unit with data retention and management procedures.
Director of Corporate Communications	Communications	Managing the personal data destruction process in accordance with the periodic destruction schedules and ensuring the compliance of his/her unit with data retention and management procedures.
Chief of IT Services	IT Services	Managing the personal data destruction process in accordance with the periodic destruction schedules and ensuring the compliance of his/her unit with data retention and management procedures.
Accounting Manager	Accounting Unit	Managing the personal data destruction process in accordance with the periodic destruction schedules and ensuring the compliance of his/her unit with data retention and management procedures.
Operations	Oil Drilling Facilities	Managing the personal data

		destruction process in accordance with the periodic destruction schedules and ensuring the compliance of his/her unit with data retention and management procedures.

DATA RETENTION AND DELETION SCHEDULES

* Updates can be made on these retention periods if needed.

Data Retention and Deletion Schedules

TYPE OF DATA	RETENTION PERIOD	DETRUCTION DATE
Contract Preparation	10 years	First scheduled periodic destruction period following the expiry of the storage period.
Employment	10 years after the termination of labor contract	First scheduled periodic destruction period following the expiry of the storage period
Employee Personal File (Human Resources): Name, Surname, ID number, Photo, Residence Certificate, social security Service Statement, Military Discharge, Postponement or Exemption Certificate, Telephone, e-mail, Diploma, Education Certificates, Driver's License, Job Application Form, Foreign Language Knowledge Details, Criminal Record Certificate, Union Membership Information, Association / Foundation Information, Family Status Notification Form, Health Report, employee paid leave Forms	10 years after the termination of labor contract	First scheduled periodic destruction period following the expiry of the storage period
Personal File, Social Security Information (Human Resources): Name Surname, ID Number, Employment Admission and Discharge Notifications, Employment Admission and Discharge Protocol, Labor Contract	10 years	First scheduled periodic destruction period following the expiry of the storage period

Minimum Living Allowance (Human Resources): ID NUMBER, Name Surname,	10 years	First scheduled periodic destruction period following the expiry of the storage period
Annual Leave Advance and Salary Advance File (Human Resources): Enrollment Number, Name Surname, Bank Account Number	10 years	First scheduled periodic destruction period following the expiry of the storage period
Payroll, Scoring, Salary, Monthly Service Statement, Sheet Payroll: Name Surname, ID Number, Attendance Control Form, Payroll, Monthly Insurance Premium Declarations	10 years	First scheduled periodic destruction period following the expiry of the storage period
Student Aid (Human Resources): Name, Surname, Address, ID Number, Photo, School, Identity Information	10 years	First scheduled periodic destruction period following the expiry of the storage period
Correspondence (Human resources) Address, ID Number, Name Surname	10 years	First scheduled periodic destruction period following the expiry of the storage period
Intern File (Human Resources): Name, Surname, Address, School, Identity Information	10 years	First scheduled periodic destruction period following the expiry of the storage period
Judicial proceedings and debt collection information about employees (Human Resources): Name, Surname, Address, Identity Information	10 years after the termination of labor contract	First scheduled periodic destruction period following the expiry of the storage period
Occupational Safety and Environmental System Audit File Credential, Communication, Training, Health Certificate	15 years	First scheduled periodic destruction period following the expiry of the storage period
Union Dues File (Human Resources): Name Surname, ID Number, Bank Account Number, Affiliated Union	10 years	First scheduled periodic destruction period following the expiry of the storage period
Information on company founders and board of directors	10 years	First scheduled periodic destruction period following the expiry of the storage period
Accident Reports	10 years	First scheduled periodic destruction period following the expiry of the storage period
Meeting / training attendance	2 years	First scheduled periodic

reports		destruction period following the expiry of the storage period
Service records: records kept during the activity (control forms, duty station books, visitor log book, vehicle entry log book, record book, weapon handover book, lost / found item form, etc.)	1 year after the termination of labor contract	First scheduled periodic destruction period following the expiry of the storage period
Accounting records (Receipt Information Regarding the Payment Made with the Invoice issued byt he Sellers; The Invoice Information the Company issues to the Customers and the Information of the Payments Made to Us, Name Surname, Address, Telephone, ID Number, Bank Account Information	10 years	First scheduled periodic destruction period following the expiry of the storage period
Job Applications (Human Resources) Name, Surname, Address, School, Identity Information	2 years	First scheduled periodic destruction period following the expiry of the storage period
Current Account Financial Information for Individual Firms (Accounting): Name Surname, Identity Number, Bank Account Information, Address	10 years	First scheduled periodic destruction period following the expiry of the storage period
Insurance Policies (Accounting): Name Surname, Identity Number, Family Information	10 years	First scheduled periodic destruction period following the expiry of the storage period
Correspondence (Accounting): Name Surname, Identity Number, Bank Account Information, Phone, Address	10 years	First scheduled periodic destruction period following the expiry of the storage period
Invoices (Accounting): Name Surname, Identity Number, Bank Account Information	10 years	First scheduled periodic destruction period following the expiry of the storage period
Bank Instructions (Accounting): Name Surname, Identity Number, Bank Account Information	10 years	First scheduled periodic destruction period following the expiry of the storage period
Debt Collection Tracking (Accounting): Identity Information, Address	10 years	First scheduled periodic destruction period following the expiry of the storage period
Market Payments (Accounting): Identity Information, Identity Number, Bank Account Information, Address	10 years	First scheduled periodic destruction period following the expiry of the storage period
Contracts (Purchase): Full Name, Business Address, E-mail	10 years	First scheduled periodic destruction period following the

Address, ID Number, Telephone Number, Fax Number, Tax Number, Tax Office Name, Trade Registry Number, Nationality, Criminal Convictions and Security Measures		expiry of the storage period
Company Promotion Files (Purchase): Business Address, E-mail Address, Identity Number, Telephone Number, Fax Number, Tax Number, Tax Office Name, Trade Registry Number, Nationality	10 years	First scheduled periodic destruction period following the expiry of the storage period
Correspondence (Purchase): Name Surname, Identity Number, Address, Phone, Fax	10 years	First scheduled periodic destruction period following the expiry of the storage period
Progress Payments (Technical Affairs): Name Surname, address, Identity information, Photograph, Telephone, E-mail, Signature circular, Power of Attorney, payment information, insurance information and declaration of employment, schools where education (Diploma), certificate information, driver's license, experience information (professional association registration certificate) annual leave, sick report, medical report, undertaking, Salary Payment Receipts, Bank Account Information, Scoring	10 years	First scheduled periodic destruction period following the expiry of the storage period
Offers (Technical Affairs): Name, Surname, address, Identity information, Photograph, Telephone, E-mail, Signature circular, Power of Attorney, payment information, insurance information and declaration of employment, schools where education (Diploma), certificate information, driver's license, experience information (professional association registration certificate)	10 years	First scheduled periodic destruction period following the expiry of the storage period
Subcontractor Files: Identity Information, Signature Circular,	10 years	First scheduled periodic destruction period following the

Telephone, Fax, Address		expiry of the storage period
Customer Complaints and Responses (Press and Public Relations): Name Surname, ID Number, Address, Phone	10 years	First scheduled periodic destruction period following the expiry of the storage period
Freedom of Information Requests and Petitions(Press and Public Relations): Name Surname, Identity Number, Address, Telephone	10 years	First scheduled periodic destruction period following the expiry of the storage period
Seminar (Press and Public Relations): Name Surname, Address, Photo	2 years	First scheduled periodic destruction period following the expiry of the storage period
Advertising and News (Press and Public Relations): Name Surname, Address, Photograph	2 years	First scheduled periodic destruction period following the expiry of the storage period
Litigation, Debt Enforcement Proceedings, Mediation, Arbitration Files (Legal): Identity information, Contact information, Career Information, Education information, Family members information, Residence, Health report, Work accident report, Salary information	10 years	First scheduled periodic destruction period following the expiry of the storage period
Personal File Health Section (Workplace Physician) Note: upon the termination of labor contract Workplace Physician records following data: (Identity information, education, address information, occupation, previous job, jobs, work places, background (blood type, congenital / chronic diseases, immunization), family history (mother-father-sibling-child any Does the worker suffer from any illness?), medical history (surgery, occupational accident, occupational diseases, disability, Is there any treatment, alcohol use, smoking) physical examination, laboratory findings, photograph)? Relevant documents are delivered to the archives to be placed in the personnel file	15 years – 40 years	First scheduled periodic destruction period following the expiry of the storage period

PERIODIC DESTRUCTION SCHEDULES

The Company destroys personal data in the first periodic destruction operation following the date when the obligation to destroy personal data arose. In this context, the storage period of our Company's personal data is 10 (ten) years, and the data that are obligatory to be kept for certain periods within the scope of legal requirements are processed limited to the periods specified in the law. In the event of a legal obligation to destroy personal data, the Company subjected the personal data to the destruction process in 6 (six) months periods. The aforementioned period does not exceed the maximum periodic destruction period specified in Article 11 of the Regulation in any case and condition. Periodic destructions are scheduled to be done in June and December of every calendar year.

PUBLISHING AND STORAGE OF THE POLICY:

The policy shall be published in two different media as wet signed (printed paper) and electronically, and disclosed to the public on the website. The printed paper copy shall be kept in the Data Retention and Management Policy file.

ENFORCEMENT and AMENDMENTS:

This Policy enters into force on the date of its publication. The policy may be updated from time to time in order to reflect new conditions and provisions of legislation. The updated Policy text will enter into force on the date it is published at "http://aladdinmiddleeast.com/TR.aspx".

The policy shall be reviewed as needed and can be modified at any time and without previous notice.