Abdul Latif Jameel FINANCE

PERSONAL DATA PROTECTION POLICY

تمكّن
Empowering you

CONTENTS

Personal Data Protection Policy

1. INTRODUCTION

Abdul Latif Jameel United Finance Company (ALJUF) is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviors of ALJUF employees and Third Parties in relation to the collection, use, retention, transfer, disclosure, destruction and breach of any Personal Data belonging to ALJUF Data Subject.

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organizations may process Personal Data. ALJUF through its Data Management Office (DMO) is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose ALJUF to complaints, regulatory action, fines and/or reputational damage.

ALJUF management is fully committed to ensuring continued and effective implementation of this policy and expects all ALJUF Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action in accordance with ALJUF HR policies and procedures

The National Data Management Office (NDMO) requires this policy.

2. SCOPE

This policy applies to all ALJUF Entities where a Data Subject's Personal Data is processed:

- In the context of the business activities of the ALJUF Entity.
- For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by ALJUF.
- To actively monitor the behavior of individuals. Monitoring the behavior of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:
    - Taking a decision about them.
    - Analyzing or predicting their personal preferences, behaviors and attitudes.
    - As required by law and government entity.

This policy applies to all processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy has been designed to establish a baseline standard for the processing and protection of Personal Data by all ALJUF Entities. Where the law imposes a requirement, which is stricter than imposed by this policy, the requirements in the law must be followed. Furthermore, where the law imposes a requirement that is not addressed in this policy, the relevant law must be adhered to.
If there are conflicting requirements in this policy and the law, please consult with Personal Data Protection Officer (PDPO) for guidance.

3. DEFINITIONS

Employee	An individual who works part-time or full-time for ALJUF under a contract of employment, whether verbal or written, express or implied, and has recognized rights and duties. Includes temporary employees and independent contractors.
Third Party	An external organization with which ALJUF conducts business and is also authorized to, under the direct authority of ALJUF, process the Personal Data of ALJUF Data Subjects, Employees, Suppliers, Service Providers and Contractors etc.
Personal Data	Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.
Contact	Any past, current or prospective ALJUF customer.
Identifiable Natural Person	Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
ALJUF	Abdul Latif Jameel United Finance Co., including subsidiaries and joint ventures over which ALJUF exercise management control.
Data Subject	The identified or Identifiable Natural Person to which the data refers.
process, processed, processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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 Protection	The process of safeguarding Personal Data from unauthorized or unlawful disclosure, access, alteration, processing, transfer or destruction.
Data Protection Authority	An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in the NDMO standard.
Data processors	A natural or legal person, Public Authority, Agency or other body which processes Personal Data on behalf of ALJUF.

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.
Special Categories of Data	Personal Data pertaining to or revealing racial, ethnic or tribal origin, political ideology,, religious or philosophical beliefs, organizational membership; data concerning health or biometric data, criminal record, credit record, location tracking data, status of legitimacy (Known / Unknown parent(s))
Profiling	Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyze or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behavior, location or movement.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Encryption	The process of converting information or data into code, to prevent unauthorized access.
Anonymization	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

4. GOVERNANCE

4.1. Policy Dissemination & Enforcement

The management team of ALJUF must ensure that all ALJUF employees responsible for the processing of Personal Data are aware of and comply with the contents of this policy.

In addition, ALJUF will make sure all Third Parties engaged to process Personal Data on their behalf (i.e. their Data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by ALJUF.

4.2. Data Protection By Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

ALJUF must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has

responsibility. The subsequent findings of the DPIA must then be submitted to the Data Protection Officer for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Management Office (DMO) to assess the impact of any new technology uses on the security of Personal Data.

4.3. Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by ALJUF in relation to this policy, the Internal Audit department will carry out an annual Data Protection Compliance Audit for all such Entities. Each audit will assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities.
  - Raising awareness.
  - Training of Employees.
- The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights.
  - Personal Data transfers.
  - Personal Data incident management.
  - Personal Data complaints handling.
- The level of understanding of Data Protection policies and Privacy Notices.
- The accuracy of Data Protection policies and Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data processor activities.
- The adequacy of procedures for redressing poor compliance and Personal Data breaches.

The DMO with support from the Personal Data Protection Officer (PDPO), in cooperation with key business stakeholders from ALJUF, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable period. Any major deficiencies identified will be reported to and monitored by the ALJUF Data Management Committee.

5. DATA PROTECTION PRINCIPLES

ALJUF has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

- **Principle 1: Lawfulness,** Fairness and Transparency Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, ALJUF must tell the Data Subject what processing will occur (transparency), the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Personal Data Protection regulation (lawfulness).

- **Principle 2: Purpose Limitation** Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means ALJUF must specify exactly what the Personal Data collected will be used for and limit the processing of that Personal Data to only what is necessary to meet the specified purpose.
- **Principle 3: Data Minimization** Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means ALJUF must not store any Personal Data beyond what is strictly required.
- **Principle 4: Accuracy** Personal Data shall be accurate and, kept up to date. This means ALJUF must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.
- **Principle 5: Storage Limitation** Personal Data shall be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. This means ALJUF must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject. Data retention is governed by various laws, some of which stipulates the retention period to be ten years beyond the conclusion of a contract.
- **Principle 6: Integrity & Confidentiality** Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage. ALJUF must use appropriate technical and organizational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.
- **Principle 7: Accountability** The Data Management Office (DMO) shall be responsible for, and be able to demonstrate compliance. This means ALJUF must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

6. DATA COLLECTION

6.1. Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or entities.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A Saudi law expressly provides for the collection, processing or transfer of the Personal Data.

Where it has been determined, that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data.
- At the time of first communication if used for communication with the Data Subject.
- At the time of disclosure if disclosed to another recipient.

6.1.1. Data Subject Consent

ALJUF will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, ALJUF is committed to seeking such Consent.

The Personal Data Protection Officer (PDPO), in cooperation with Data Management Office (DMO), Data processor(s), and other relevant business representatives, shall establish a system for obtaining and documenting Data Subject Consent for the collection, processing, and/or transfer of their Personal Data. The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent.
- Ensuring the request for consent is presented in a manner that is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

6.1.2. Data Subject Notification

ALJUF will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the processing of their Personal Data.

When the Data Subject is asked to give Consent to the processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information.
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given verbally, electronically or in writing. If given verbally, the person making the disclosures should use a suitable script or form approved in advance by the Personal Data Protection Officer (PDPO). The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

6.1.3. External Privacy Notices

Each external website provided by ALJUF will include an online 'Privacy policy' and an online 'Cookie policy' fulfilling the requirements of applicable law. Refer to ALJUF Privacy policy and Cookies policy for guidance. All Privacy and Cookies policies must be approved by the DMO supported by the Personal Data Protection Officer (PDPO), and the Board of Directors prior to publication on any ALJUF external website.

6.2. Data Use

6.2.1. Lawfulness of processing

ALJUF will only process personal data in accordance this policy. All processing undertaken by ALJUF will be in line with the purposes for processing stated in the next paragraph.

6.2.2. Data processing

ALJUF uses the Personal Data of its employees and customers and suppliers for the following broad purposes:

- The general running and business administration of ALJUF.
- To provide services to ALJUF customers and employees.
- The ongoing administration and management of customer services.
- To share with government agencies / or their appointed agencies whenever required.
- To share with local credit bureaus.
- To offer employment.
- To offer promotions of products and services and other marketing benefits based on customer behavior and outcomes of internal data analytics.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by ALJUF to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that ALJUF would then provide their details to Third Parties for marketing purposes.
ALJUF will process Personal Data in accordance with all applicable laws and applicable contractual

obligations. More specifically, ALJUF will not process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the processing of their Personal Data for one or more specific purposes.
- processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- processing is necessary for compliance with a legal obligation to which the ALJUF is subject.
- processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- processing is necessary for the performance of a task carried out in the public interest.
- processing is necessary for the purposes of the legitimate interests pursued by ALJUF or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Compliance Officer before any such processing may commence.
In any circumstance where Consent has not been gained for the specific processing in question, ALJUF will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the ALJUF.
- The nature of the Personal Data, in particular whether Special Categories of Data are being processed, or whether Personal Data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further processing, which may include Encryption or Anonymization.

6.2.3. Special Categories of Data

ALJUF will only process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to Personal Data that has already been made public by the Data Subject.
- The processing is necessary for the establishment, exercise or defense of legal claims.
- The processing is specifically authorized or required by law.
- The 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.

In any situation where Special Categories of Data are to be processed, prior approval must be obtained from the Personal Data Protection Officer (PDPO) and the basis for the processing clearly recorded with the Personal Data in question.

Where Special Categories of Data are being processed, ALJUF will adopt additional protection measures. ALJUF may also adopt additional measures to address local custom or social expectation over the processing of Special Categories of Data. ALJUF will also abide the Saudi laws and regulations.

6.2.4. Children's Data

As a given, Saudi Law defines children as Data Subjects under the age of 18. Since children are unable to consent to the processing of their Personal Data, consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other legal grounds, Consent need not be obtained from the child or the holder of parental responsibility.

ALJUF does not offer any products or services directly to children. Children dependents of employees are offered medical insurance as a fringe benefit based on their dependency on their ALJUF-employed parent.

ALJUF collects the minimum and necessary information on the children of its employees for the soul purpose of providing medical insurance to the employee and his/her dependent family. The information is collected only directly from the parent or legal guardian of the child and includes the following:

a. Patronymic name of the child
b. His/her ID number
c. Date of birth
d. Place of birth
e. No other information is collected

Should ALJUF foresee a business need for obtaining parental consent directly from a child, guidance and approval must be obtained from the Personal Data Protection Officer (PDPO) before any processing of a child's Personal Data may commence.
ALJUF does not knowingly collect personally identifiable information from anyone under the age of 18. If a parent or guardian becomes aware that his Child has provided ALJUF with Personal Data, they should contact ALJUF. If ALJUF becomes aware that it has unknowingly collected Personal Data from children without verification of parental consent, ALJUF will take steps to remove that information from their servers.

6.2.5. Data Quality

ALJUF will adopt all necessary measures to ensure that the Personal Data it collects, and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject. The measures adopted by ALJUF to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, insofar as:
    - a law prohibits erasure.
    - erasure would impair legitimate interests of the Data Subject.
    - the Data Subject disputes that their Personal Data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

6.2.6. Profiling & Automated Decision-Making

ALJUF will only engage in Profiling and automated decision-making where it is necessary to enter into or to perform, a contract with the Data Subject or where it is authorized by law and / or where consent is obtained from the Data Subject.
Where ALJUF utilizes Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases, the Data Subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.

- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out.

ALJUF must also ensure that all profiling and automated decision-making relating to a Data Subject is based on accurate data.

6.2.7. Digital Marketing

As a rule, ALJUF will not send promotional or direct marketing material to ALJUF Contact through digital channels such as mobile phones, e-mail and the Internet, without first obtaining their Consent. When ALJUF wishes to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject, it must first have it approved by the Personal Data Protection Officer (PDPO).

Where Personal Data processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the Data Subject puts forward an objection, digital marketing related processing of their Personal Data must cease immediately, and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

6.3. Data Retention

To ensure fair processing, Personal Data will not be retained by ALJUF for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which ALJUF needs to retain Personal Data is set out in the ALJUF 'Data Retention Policy'. This considers the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

6.4. Data Protection

ALJUF will adopt physical, technical, and organizational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorized alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted ALJUF is provided in the ALJUF 'Information Security Policy'. A summary of the Personal Data related security measures is provided below:

- Prevent unauthorized persons from gaining access to data processing systems in which Personal Data are processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorizations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorization.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data processor, the data can be processed only in accordance with the instructions of the DMO.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is processed separately.
- Ensure that Personal Data is not kept longer than necessary.

6.5. Data Subject Requests

The DMO with support from the Personal Data Protection Officer (PDPO) will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure.
- Opt-out of future communications

If an individual makes a request relating to any of the rights listed above, ALJUF will consider each such request in accordance with all applicable Personal Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed unnecessary or excessive in nature.
Data Subjects are entitled to obtain, based upon a request made in writing to ALJUF and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject.

- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to:
    - object to processing of their Personal Data.
    - lodge a complaint with the Saudi Central Bank or other authorities.
    - request rectification or erasure of their Personal Data.
    - request restriction of processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the PDPO, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorized legal representative.
Data Subjects shall have the right to require ALJUF to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.
If ALJUF cannot respond fully to the request within 30 days, the DMO shall nevertheless provide the following information to the Data Subject or their authorized legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications that will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the ALJUF individual who the Data Subject should contact for follow up.
- Data Subject requests will be available through ALJUF website

It should be noted that situations might arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

6.6. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If ALJUF processes Personal Data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If ALJUF receives a request from a court or any regulatory or law enforcement authority for information relating to ALJUF Contact, the recipient must immediately notify ALJUF Legal Officer and the Personal Data Protection Officer (PDPO) who will provide comprehensive guidance and assistance.

6.7. Data Protection Training

All ALJUF employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, ALJUF will provide regular Data Protection training and procedural guidance for their staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles above.
- Each Employee's duty to use and permit the use of Personal Data only by authorized persons and for authorized purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorized person.
- Securely storing manual files, print outs and electronic storage media.
- The need to obtain appropriate authorization and utilize appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.
- Proper disposal of Personal Data by using secure shredding facilities.
- Any special risks associated with particular departmental activities or duties.

6.8. Data Transfers

ALJUF will not transfer Personal Data to Third Party recipients located in another country without approval of the regulatory authority.

ALJUF may only transfer Personal Data to third parties located and operating within the borders of the Kingdom and where one of the transfer scenarios listed below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is necessary for the establishment, exercise or defense of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

6.8.1. Transfers to Third Parties

ALJUF will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where Third Party processing takes place, ALJUF will enter into, in cooperation with the Personal Data Protection Officer (PDPO), an appropriate agreement with the third party to clarify each party's responsibilities in respect to the Personal Data transferred. The agreement must require the Data processor to protect the Personal Data from further disclosure and to process only Personal Data in compliance with ALJUF instructions. In addition, the agreement will require the Data processor to implement appropriate technical and organizational measures to protect the Personal Data as well as procedures for providing notification of Personal Data breaches ALJUF should create a standard agreement to be used as a baseline template.

When ALJUF outsource services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will process Personal Data on its behalf. ALJUF will make sure to include, in cooperation with the Personal Data Protection Officer (PDPO), adequate provisions in the outsourcing agreement for such processing and transfers. ALJUF will create an outsourcing agreement that will be used as a standard template for such instances.

The Personal Data Protection Officer (PDPO) and/or the Internal Audit shall conduct regular audits of processing of Personal Data performed by Third Parties, especially in respect of technical and organizational measures they have in place. Any major deficiencies identified will be reported to and monitored by ALJUF Data Management Committee.

6.9. Complaint Handling

Data Subjects with a complaint about the processing of their Personal Data should put forward the matter in writing to the PDPO. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The PDPO will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the PDPO, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Supervisory Authority within the applicable jurisdiction.

6.10. Breach Reporting

Any individual, who suspects that a Personal Data breach has occurred due to the theft or exposure of Personal Data, including children's data, must immediately notify the DMO providing a description of what occurred. Notification of the incident can be directed in the first instance to the PDPO.

The DMO and Personal Data Protection Officer (PDPO) will investigate all reported incidents to confirm whether a Personal Data breach has occurred. If a Personal Data breach is confirmed, the DMO with support from the PDPO will follow the relevant authorized procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data breaches and breaches of children's data, ALJUF Legal and Compliance Departments along with Cyber Security Department, to coordinate, manage and respond to the Personal Data breach. In accordance with the relevant authorized procedure, the response may include notifying the regulators.

7. POLICY MAINTENANCE

All inquiries about this policy, including requests for exceptions or changes should be directed to the Chief Data Officer (CDO).

7.1. Publication

This policy shall be available to all ALJUF Employees through the ALJUF Intranet or via alternative means as deemed appropriate by the DMO.

7.2. Effective Date

This policy is effective as of December 2022 ,22.

7.3. Revisions

The DMO with the advice of the Personal Data Protection Officer (PDPO) is responsible for the maintenance and accuracy of this policy. Notice of significant revisions shall be provided to ALJUF Employees through the Human Resources department. Changes to this policy will come into force when published on ALJUF Intranet.

8. RELATED DOCUMENTS

ALJUF Cookie Policy
ALJUF Privacy Policy

Abdul Latif Jameel
FINANCE

ALJUF PERSONAL DATA PROTECTION POLICY

Thank You

تمكّن
Empowering you