Data Protection Policy

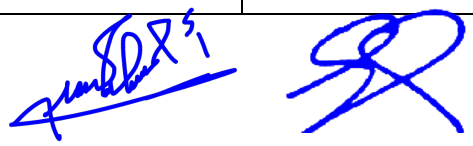
v1.0

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi



Document Change History Information			
Author	Date	Version	Change Description

Contents

Document Control Information 2
1. Introduction 4
2. Scope ofApplication 4
3. Key Definitions 4
4. Core Principles for Personal Data Protection 5
5. Governance of Personal Data Protection and Compliance with Data Protection Regulations 5
6. Disclosure of Personal Data 6
7. Collection of Personal Data 6
8. Controls for Processing Personal Data Purposes ofProcessing 8
9. Record of Personal Data Processing 9
10. Storage of Personal Data 10
B. Authorized Access 10
C. Time Limits 10
11. Sharing Personal Data with External Parties 10
B. Third-Party SecurityProcedures 10
12. Credit DataProtection 11
13. Health DataProtection 11
14. Anonymization 11
15. Data SubjectRights 12
16. Security Measures for Data Protection 12
B. Organizational Measures 12
17. Compliance 13
B. Compliance Review 13
18. Withdrawal ofConsent 13
19. Impact Assessment 13
20. Incident and Breach Management Incident Response Plan 14
21. Training and Awareness 15
22. Data Disposal(Destruction) 16
23. Policy Updates and Amendments 17

1. Introduction

The purpose of this policy is to clarify how the controller handles the personal data it collects and to provide guidelines and procedures to ensure the
protection of that data in accordance with the best standards and national laws. The company seeks to enhance transparency and accountability in managing personal data, thereby building trust between the company and the individuals it serves.

2. Scope of Application

This policy applies to all personal data collected by the controller or its contracted parties, and it includes all employees, contractors, and external partners who handle personal data.

3. Key Definitions

A. **Controller**: The entity that determines the purposes and means of processing personal data. In this case, the company is the controller responsible for
collecting, processing, and protecting personal data.

B. **Personal Data**: Personal data means any information related to a natural person that can be used to identify them directly or indirectly, such as name, ID number, address, email, etc.

C. **Public Data**: This data is available to the public and does not require permissions to access. Such data is usually non-sensitive.

D. **Restricted Data**: Data that requires specific controls for access but is not highly sensitive.

E. **Confidential Data**: Data that is highly sensitive and must be protected from unauthorized access.

F. **Sensitive Data**: Data that contains personal or confidential information and whose disclosure could violate privacy or harm the individual or entity.

G. **Critical Data**: Data whose disclosure or manipulation could have serious negative impacts on national or economic security.

H. **Credit Data**: Credit data refers to financial and personal information related to an individual's or entity's credit transactions and history.

I. **Health Data**: Information related to an individual's health, including any

information concerning their health condition, diagnoses, treatments received, or medical records in general.

4. Core Principles for Personal Data Protection

A. **Transparency**: Personal data is collected and processed legally and transparently in accordance with applicable laws and regulations.

B. **Data Minimization**: Collect only the personal data necessary to achieve the stated objectives.

C. **Accuracy**: Ensure that personal data is accurate and up-to-date, enabling individuals to correct any inaccuracies.

D. **Limited Storage**: Retain personal data only for as long as necessary for the purposes for which it was collected.

E. **Information Confidentiality Protection**: Protect data from unauthorized access, loss, alteration, or disclosure.

5. Governance of Personal Data Protection and Compliance with Data Protection Regulations

A. **Governance Model Documentation**: Adopt a plan for the governance of personal data in accordance with the data protection regulations and their provisions. The plan should include clear mechanisms in the form of multiple policies covering all required aspects and aimed at organizing the process of personal data processing in compliance with national laws.

B. **Defining Roles and Responsibilities**: Policy documents should define roles and responsibilities related to personal data governance, with a clear
distribution of tasks for each entity or employee, ensuring each role contributes to full compliance with the regulations.

C. **Reporting Lines**: Clear and defined reporting lines must be established to allow continuous monitoring of compliance with the data protection regulations and their executive provisions. These lines contribute to supporting transparency within the organization and facilitating reporting of any violations or challenges.

D. **Conflict Resolution**: In the event of internal conflicts regarding the implementation of the data protection regulations, the organization must adopt effective mechanisms to identify and resolve these conflicts promptly and
efficiently, ensuring consistent and coherent policy application in line with regulatory requirements.

6. Disclosure of Personal Data

A. Disclosure of data collected from publicly available sources must comply with the regulations and their provisions.
B. When disclosing data, it must:

- Be related to a specific and clear purpose.
- Maintain the privacy of the data subject.
- Be limited to the minimum necessary data to achieve the purpose.
  C. When disclosing to a public entity for security or health purposes:
- The request must be documented accurately.
- The type of data to be disclosed must be specified.
  D. If the data is related to someone other than the data subject, it must:
- Balance the rights of individuals.
- Anonymize the identity of the other person where possible.
  E. All disclosures must be documented in special records.

7. Collection of Personal Data

A. Sources of Personal Data: The controller collects personal data from several sources, including:

- The data subject directly when services are provided, and they must be informed of the following:
  - The name of the controller and contact details.
  - Data Protection Officer details, if available.
  - The legal basis and purpose of data collection.
  - The retention period of the data or the criteria for determining it.
  - The rights of the data subject and how to exercise them.
  - How to withdraw consent.
  - Whether data collection is mandatory or optional.
- Third parties such as business partners.
- Publicly available sources, as necessary.
  B. Consent

- Consent must be obtained from data subjects in a clear and unambiguous manner.
- Consent must be explicit if the data being processed is sensitive or credit-related, or if decisions are to be made based on automated processing of personal data.
- The purposes of collection and processing must be clarified before obtaining consent.
- Consent must be documented in a technical means that can be referenced in the future.
- Independent consent must be obtained for each purpose of collection and processing.
- Consent must come from a fully capable data subject or their legal guardian.
- If the data subject is minor or incapacitated, the legal guardian has the right to:
    - Exercise the rights of the data subject as per the regulations and provisions.
    - Consent to the processing of their data in accordance with the regulations.
      When processing data of minors or incapacitated persons:
    - Verify the validity of the legal guardianship.
    - Ensure that no harm is inflicted on the interests of the data subject.
    - Enable the data subject to exercise their rights when they reach legal capacity.
      C. Collection of Sensitive Data: Processing sensitive data requires specific consent and is collected only when necessary, with the highest levels of protection applied.
      D. Collection of Minimum Data
- The controller must collect the minimum personal data necessary to achieve the purpose of processing.
- The data must be directly related to the processing purpose.
- Due diligence must be taken to ensure unnecessary data is not collected.

- The immediate need for this data must be identified and recorded, and the use of this data must cease when it is no longer necessary.
  E. Collection of Data from Non-Subjects Directly
- Processing must be necessary and proportionate to the specified purpose, and must not affect the rights and interests of the data subject; the controller must retain evidence of the inability to contact the data subject or the difficulty in reaching them.
- The data subject must be informed about the data collection process within no more than thirty days.
- When collecting data from publicly available sources, it must be done in a legal manner.
- In case of processing, anonymization must be considered as per Article 9 of the executive regulations of the Personal Data Protection Law.

8. Controls for Processing Personal Data Purposes of Processing

- Personal data is processed for:
  - Providing services agreed upon with partners.
  - Administrative purposes within the company, such as hiring and evaluation.
  - Compliance with regulatory laws.
    B. Processing Restrictions
- Personal data is used only for the specified and announced purposes, and data subjects will be informed if there is additional processing for another purpose.
- The use of data for unlawful purposes or in violation of the rights of data subjects isprohibited.
  C. Security Measures During Processing
- Encryption techniques are applied when processing sensitive data.
- Specific roles and permissions for accessing personal data are allocated.
- Access activities are monitored to prevent any unauthorized access or use.

D. In the case of selecting a processing entity, the controller must include the following in the agreement with the processing entity:

- The controller issues specific instructions for the data to the processing entity, and in case of non-compliance, the processing entity must notify the controller in writing and promptly.
- The purpose of processing.
- The duration of processing.
- The processing entity's commitment to notify the controller in the event of personal data leakage without delay.
- Clarification of whether the processing entity is subject to regulations in other countries and the impact of that on its compliance with the applicable regulations in the Kingdom.
- The processing entity should not be required to obtain prior consent for mandatory disclosure from the controller, and the first must notify the second about the disclosure.
- The controller must ensure the processing entity's compliance with data-specific regulations and laws periodically, and the former has the right to engage a third party to verify that.
- The processing entity is treated as the controller in the event of violating the data regulations specific to the controller.

E. In the case of the processing entity engaging a third party:

- Ensure the integrity and security of the processed data are not compromised.
- Obtain prior consent from the controller for engaging the third party.

9. Record of Personal Data Processing

Detailed records must be maintained regarding the processing of personal data, and this record should be kept for (five years) after the processing is completed. The processing entity must provide these records upon request from data subjects and relevant authorities. The records include:

A. The identity of the person responsible for processing the data.
B. Details of the controller.
C. Entities authorized to access this data.
D. Description of the category of data.

E. The purpose of collecting this data.
F. Duration of data retention.

10. Storage of Personal Data

A. Digital Platform and Cloud Storage

- Personal data must be stored on secure systems that ensure data protection from cyber-attacks.
- In the case of using cloud storage services, it must be ensured that the provider complies with security and data protection standards.

B. Authorized Access

- A strict policy is applied to ensure that only authorized individuals can access personal data.
- Every access to the data must be recorded and documented to ensure transparency.

C. Time Limits

- Personal data is retained only for the necessary periods, and after the need for it has passed, it must be securely destroyed.

11. Sharing Personal Data with External Parties

A. Data Sharing Agreements

- Personal data shall not be shared with external parties except based on formal agreements that ensure prior approvals, confidentiality of information, and compliance with laws.
- The agreements must include clauses about data protection and compliance with legal requirements.

B. Third-Party Security Procedures

- Security measures of external parties are evaluated before signing agreements.
- Compliance is monitored periodically through regular audits.

12. Credit Data Protection

A. **Protective Measures**: The controller must implement organizational, technical, and operational measures to ensure the protection of credit data from any unauthorized use, ensuring it is accessed only for the purposes for which it was collected and preventing its leakage.
B. **Compliance with Central Bank Requirements**: The controller must adopt and apply the requirements and controls issued by the Saudi Central Bank and other relevantauthorities.
C. **Data Subject Consent**: The controller must obtain the consent of the data subject and inform them when there is any request for disclosure of their credit data.

13. Health Data Protection

If the controller needs to handle health data, the following must be ensured:
A. **Protective Measures**: Implement organizational, technical, and operational measures to protect health data from unauthorized use, or use for purposes other than those for which it was collected, and ensure the privacy of data subjects.
B. **Adoption and Application of Requirements**: Issued by the Ministry of Health, the Saudi Health Council, the Saudi Central Bank, the Health Insurance Council, and other relevant authorities.
C. **Incorporation of Provisions**: Include provisions from the system and its regulations in the internal policies of the controller, and clearly distribute roles and responsibilities to avoid overlap.
D. **Documentation**: Document all stages of processing health data and identify the responsible individuals for each stage.

14. Anonymization

According to the executive regulations of the Personal Data Protection Law, data that has been anonymized is not considered personal data, and the controller, when anonymizing the identity of the data subject, must ensure the following:
A. The identity cannot be re-identified.
B. Impact assessments must ensure that re-identification is not possible.
C. Necessary measures must be taken to avoid risks, with updates to technologies as developments occur.
D. Assess the effectiveness of anonymization techniques and adjust them as necessary.

15. Data Subject Rights

A. Access to Personal Data

Data subjects have the right to:

- Request access to the personal data held by the company.
- Receive information about how their data is processed.

B. **Correction and Deletion of Data**: Data subjects have the right to request correction of inaccurate personal data or deletion if it is no longer needed.

C. **Right to Object**: Individuals have the right to object to the processing of their personal data for specific purposes, such as direct marketing.

D. The controller must provide appropriate means to enable data subjects to exercise their rights, including email, text messages, national address, electronic applications, or any other official means of communication.

16. Security Measures for Data Protection

A. Technological Solutions

- Encryption techniques and firewalls are used to protect data from breaches.
- Backup solutions are implemented to preserve files from any incidents that may cause data loss.
- Recovery tests (test drills) are conducted to ensure the success and continuity of backup operations.
- Access controls are used to ensure that only authorized employees can access sensitive data.

B. Organizational Measures

- Employees are trained on data protection and raised awareness of associated risks.
- Regular reviews are conducted to ensure compliance with policies and standards.

17. Compliance

A. **Incident Response Plans**: Comprehensive incident response plans are established for data breach incidents that include notifying relevant authorities

and affected individuals.

B. Compliance Review

- The company conducts regular audits to ensure compliance with all policies and regulations related to personal data protection.
- Periodic reports are prepared to review compliance and submitted to senior management.

C. **Corrective Actions**: In case of any violations or breaches of policies, immediate corrective actions are taken, reviewing all relevant systems to ensure that incidents do not recur.

18. Withdrawal of Consent

The data subject has the right to withdraw their consent for the processing of their data at any time, notifying the controller. The controller must:

A. Provide easy procedures for withdrawing consent, making them simpler than the procedures for obtaining consent.

B. Cease processing immediately upon withdrawal.

C. Notify those to whom the data was disclosed and request its destruction. The withdrawal does not affect the legality of prior processing or processing based on other legal justifications.

19. Impact Assessment

A. The controller must prepare a written and documented assessment to evaluate the impacts and risks that may affect the data subject due to the processing of their data.

B. An impact assessment is conducted in the following cases:

- When processing sensitive personal data.

- When collecting or linking two or more sets of data from different sources.
- When processing data for minors, or incapacitated individuals, or using emerging technologies, or making decisions based on automated processing.
- When providing products or services that may significantly impact individuals' privacy.

C. The impact assessment should include the following elements:

- The purpose of processing and its legal basis.
- A description of the types of data and the scope of processing.
- The relationship between data subjects and processing entities.

D. Necessary measures must be identified to ensure that only the minimum required data is processed.

E. Evaluate potential negative impacts, whether social, financial, or otherwise.

F. Appropriate measures must be taken to prevent or mitigate risks.

G. If the assessment shows that the processing will harm individuals' privacy, these issues must be addressed, and the assessment must be revisited.

20. Incident and Breach Management Incident Response Plan

In the event of any incident related to the leakage of personal data or unauthorized access, an incident response plan must be executed.

Immediate notification to the Central Bank within 72 hours of discovering the incident.

B. The notification includes:

- A description of the data leakage incident, specifying the time, date, and manner of occurrence, and when the controller became aware of it.
- The categories and actual or approximate numbers of affected data subjects, and the type of data that was leaked.
- A description of the potential risks arising from the

incident, along with clarifying the actions taken to mitigate impacts and future measures to prevent recurrence.

C. A statement regarding whether the affected data subjects have been or will be notified of the leak.

D. If the controller is unable to provide the required information within (72) hours, it must provide it as soon as possible with justifications for the delay.

E. The controller retains a copy of the reports submitted to the relevant authority, documenting the corrective measures taken and any related documents.

F. The provisions of this policy do not affect any other obligations of the controller or processor to report leakage incidents as determined by the National Cybersecurity Authority or other applicable regulations.

G. The controller must notify the data subject without unreasonable delay if the incident could cause harm to their data or interfere with their rights.

H. The notification to the data subject must include:

- A description of the incident.
- A description of potential risks and measures taken to mitigate them.
- The name and contact details of the controller or the data protection officer.
- Recommendations or advice to avoid risks and mitigate impacts.

I. The notification must be in clear and simple language for the data subject.

J. The controller is committed to cooperating with relevant authorities to ensure the incident is addressed and necessary actions are taken to prevent recurrence.

21. Training and Awareness

A. **Training Programs**: Continuous training programs are organized for employees to raise their awareness of data protection policies and how to handle them securely.

B. **Awareness Campaigns**: Internal awareness campaigns are implemented to increase employees' understanding of how to

protect personal data and comply with policies.

C. **Performance Evaluation**: Employees' performance in handling personal data is evaluated within the framework of performance indicators to ensure
Continues improvement.

22. Data Disposal (Destruction)

A. Destruction Policy

- When personal data is no longer necessary for the purposes for which it was collected or upon the termination of the business relationship with partners, it must be securely destroyed.
- Based on the request of the data subject.
- If the data subject withdraws consent, and the consent was the sole basis for processing.
- If processing data is found to be non-compliant with regulations.
- Procedures such as permanent deletion from systems or destruction of media containing the data are used.

B. **Documentation**: All data disposal processes must be documented to ensure compliance with policies.

C. **Establishment of a Disposal Committee**: An internal committee within the company ensures the implementation of the aforementioned policy and issues a letter confirming the complete execution of the
disposal. The controller must dispose of personal data in the following cases:

D. Upon disposal, the other parties to whom the data was disclosed must be notified and requested to dispose of the data, in addition to destroying all copies, including backups, while considering regulatory requirements.

23. Policy Updates and Amendments

A. **Periodic Review**: This policy is regularly reviewed to ensure its compliance with laws and new developments in the field of data protection.

B. **Emergency Amendments**: The policy is amended immediately if necessary due to legal or regulatory changes affecting personal data protection