جامعة فهد بن سلطان
FAHAD BIN SULTAN UNIVERSITY

PERSONAL DATA PROTECTION POLICY

Policy Code:	AD-095-1
Policy Name:	Document Control Policy
Classification:	Confidential and Proprietary
Handler/Owner:	University Secretary
Date Created	December 2024
Approved by:	Board of Trustees
Date of Approval:	May 7, 2025
Review due date:	February 2028

Table of Contents

1. Preface

1.1 Objective

The objective of this Policy is to maintain a documentation of the guidelines and procedures that shall be followed at Fahad Bin Sultan University (FBSU) related to PDPL which has been adopted to regulate the processing of Personal Data. The scope of the PDPL includes. This Policy aims to guide the process owner and other related stakeholders for the guidelines.

1.2 Intended Audience

This Policy is intended to be a reference for the relevant Managers/Directors/Department Heads and Staff at the University. It is designed to assist all concerned personnel in consistently implementing relevant Guidelines and Procedures.

1.3 Deviation from Policies or Procedures

The DPO at FBSU, in coordination with Legal Department, shall be responsible for ensuring compliance with the letter and spirit of these guidelines and procedures, where any deviation shall be justified and approved by Head of Division.

- The deviation approval paper maintained is archived for future reference.
- Head of function is responsible for the archival of such document.

1.4 Clarification

All queries related to the interpretation of the policies and procedures within this Policy shall be addressed to the relevant Departmental Head.

1.5 Policy Distribution

The Policy Distribution is governed by the following points:

- This Policy is the property of FBSU, where one master-controlled copy (hard copy) shall be maintained, and a softcopy made available on the university intranet as a secured, read only non- printable document.
- The contents of this Policy shall be confidential and intended for internal use by the FBSU only.

1.6 Document Archive

The physical documents will be archived based on the following points:

- All the documentary evidence stored in box files along with transaction references.
- The Head of the function is responsible to maintain completeness of document archive in compliance with relevant Document Retention Requirements.

The digital documents will be archived based on the following points:

- All digital evidence of transactions is archived in shared folders of the university (Subject to Authorization access controls).
- Local laws are applicable with respect to the duration of document archive.

2. Policy Revision

Review and Revision of the policy shall take place after every three years by the DPO in coordination with the Legal Department or when one or a combination of conditions occur which are written in the end of this paragraph, for it is the principal way of implementing and communicating changes to the Policy, which may arise in response to the changing needs and requirements of the business. Such revisions provide flexibility in the processes and ensure that the Policy always remains relevant.

- Changes to the Policy shall be made as a result of one or a combination of the following events:
- Changes in laws, relevant regulations and related public decisions (including country laws, standards, etc.);
- Changes in functions and main activities of the FBSU where new personal data might be included;
- Changes in business processes.

The Policy revision process shall be governed by the following points:

- The objective of formalizing the manual revision process is to ensure that all amendments, additions or deletions to the Policy are properly documented and authorized/approved according to the DOA Matrix, prior to implementation.
- All the users of the manual shall be notified upon the completion of any revision or amendment of the Policy.

3. Definitions:

No.	Term	Definition
1.	Law	The Personal Data Protection Law.
2.	Regulations	The implementation Regulation of the Law.
3.	Competent Authority	The authority to be determined by a resolution of the Council of Ministers.
4.	Personal Data	Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, date of birth, addresses, contact numbers, license numbers, records, personal assets, bank and credit card

No.	Term	Definition
		numbers, photos and videos of an individual, and any other data of personal nature.
5.	Personal Data Processing	Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing, and destroying data.
6.	Data collection	The collection of Personal data by Controller in accordance with the provisions the law, either from personal data subject directly, a representative of the personal data subject, any legal guardian over the Data Subject or any other party.
7.	Destruction	Any action taken on Personal Data that makes it unreadable and irretrievable, or impossible to identify the related Data Subject.
8.	Data Disclosure	Enabling any person, other than the controller or processor, to obtain, use or access Personal Data by any means or for any purpose.
9.	Data transfer	The transfer of personal data from one place to another for processing.
10.	Publishing	Transmitting or making available any Personal Data using any written, audio, or visual means.
11.	Sensitive Personal Data	Personal Data revealing racial or ethnic origin, or religious, intellectual, or political belief, data relating to security, criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health Data, and data that indicates that one or both of the individual's parents are unknown.
12.	Genetic Data	Any Personal Data related to the hereditary or acquired characteristics of a natural person that uniquely identifies the characteristics of that person, and derived from biological sample analysis of that person, such as DNA or any other testing that leads to generating Genetic Data physiological or health.
13.	Health Data	Any Personal Data related to an individual's health condition, whether their physical, mental, or psychological condition, or related to Health Services received by that individual.
14.	Health Services	Services related to the health of an individual, including preventive, curative, rehabilitative and hospitalizing services, as well as the provision of medications.
15.	Credit Data	Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that Individual's ability to obtain and repay debts, and the credit history of that person.
16.	Data Subject	The individual to whom Personal Data relates.

No.	Term	Definition
17.	Public Entity	Any ministry, department, public institution or public authority, any independent public entity in the Kingdom, or any affiliated entity therewith.
18.	Controller	Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the Data is processed by that Controller or by the Processor. FBSU and its affiliates are defined as Controllers of the personal data.
19.	Processor	Any Public Entity, natural person or private legal person that processes Personal Data for the benefit and on behalf of the Controller.
20.	Direct Marketing	Communicate with the Data subject by any direct physical or electronic means with the aim of directing marketing material; this includes but is not limited to advertisements or promotions.
21.	Personal Data Breach	Any incident that leads to the Disclosure, Destruction, or unauthorized access to Personal Data, whether intentional or accidental, and by any means, whether automated or manual.
22.	Vital Interest	Any interest necessary to preserve the life of a Data Subject.
23.	Actual Interest	Refers to any moral or material interest of the Data Subject that Is directly linked to the purpose of Processing Personal Data, and the Processing is necessary to achieve that interest.
24.	Legitimate Interest	Refers to any necessary interest of the Controller that requires the Processing of Personal Data for a specific purpose, provided it does not adversely affect the rights and Interests of the data subject.
25.	Pseudonymization	Conversion of the main identifiers that indicate the identity of the Data Subject into codes that make it difficult to directly identify them without using additional data or information. The pseudonymized data or additional information should be kept separately, and appropriate technical and administrative controls should be implemented to ensure that they are not specifically linked to the data subject's Identity.
26.	Anonymization	Removal of direct and Indirect identifiers that indicate the identity of the Data Subject in a way that permanently makes it impossible to identify the Data Subject.
27.	Explicit Consent	Direct and explicit consent given by the Data Subject in any form that clearly indicates the Data Subject's acceptance of the Processing of their Personal Data in a manner that cannot be interpreted otherwise, and whose obtention can be proven.
28.	Company	"FBSU and its affiliates
29.	Employee	An individual who works full-time or part-time for FBSU under a contract of employment, whether verbal or written, express or implied, and has recognized rights and duties. Includes temporary employees and independent contractors.

No.	Term	Definition
30.	Third Party	An external organization with which FBSU conducts business and is also authorized to, under the direct authority of FBSU, process the Personal Data of FBSU Data Subjects, Employees, Suppliers, Service Providers and Contractors etc.

4. Introduction

During its operations, the company needs to gather, process, and use certain information about individuals. This will include clients, prospective clients, suppliers and other business contacts, employees, and prospective employees, as well as other people that we have a relationship with, may need to contact, or with whom we need to deal.

5. Why does this policy exist:

This policy provides help and guidance to our staff and managers in:

- Understanding and complying with personal data protection law and regulations and following good practices.
- Protecting the rights of staff, clients, partners, and business contacts being aware about how we use and process personal data, how we store it, how we secure it and how we delete it.
- Protecting the company against the risks of both inadvertent and intentional data breaches.

6. Scope of the policy:

6.1 PDPL shall be applied on any processing of personal data related to individuals that takes place in the Kingdom of Saudi Arabia by the Group Companies as well as any Processing of Personal Data of the individuals, employees, contractors, partners, and third parties who are located in the Kingdom and have access to or handle personal data collected or processed and/or carried out by any means on behalf of FBSU.

6.2 This also includes the data of the deceased if it would lead to them, or a member of their family being identified specifically.

6.3 This policy also 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.

6.4 FBSU and its affiliates are hereby defined as Controllers of personal data.

6.5 This policy describes the Personal Data Subjects rights and the Group obligations towards them and how this personal data must be collected, processed, transferred, handled, and stored to meet the requirements of Personal data protection law and regulations, in particular the Personal Data Protection Law (PDPL) in KSA. We recognize that not only must we comply with the principles of lawful processing of personal data, we must also be

able to demonstrate that we have done so. The principles set out below shall always be followed by the university, its employees and all those within its scope as set out below.

7. Data Protection Policy:

7.1 What is Personal Data?

7.1.1 The PDPL regulates how organizations collect, process, share and store personal data. Personal data is any data or information, regardless of its source or form, relating to an identified or identifiable living individual. It is information which enables that person to be identified, directly or indirectly, and may include:

- First name and last name,
- Personal identification number such as national identity,
- Address
- Contact number(s).
- License numbers
- Records
- Personal assets
- Age
- Location data
- Bank account number
- Credit card number
- Health data
- Images or photos
- Videos and biometric identifiers
- Any other data of personal nature etc.

7.1.2 These rules apply to all data stored in any manner, including both hard copies and electronically.

7.2 Sensitive Personal Data or 'Special Category Data'

7.2.1 The PDPL regulates how organizations collect, process, share and store personal data. Personal data is any data or information, regardless of its source or form, relating to an identified or identifiable living individual. It is information which enables that person to be identified, directly or indirectly, and may include:

- Race
- Ethnicity
- Criminal and security data including convictions and offenses
- Religion
- Intellectual or political belief
- Genetics data
- Biometrics used for identification purposes

- Health data
- Data that indicates that one or both of the individuals' parents are unknown.

7.2.2 There are several strict rules about the processing of this kind of data, and the kinds of situations in which it is legitimate to process it, it shall be collected directly from the Data Subject and the data controller needs the data subject's explicit written consent to do so or a clear legal basis. We will never disclose such data to any third party unless legally obliged to do so, and then only to appropriate authorities as required by law, it is not allowed to rely on a lawful basis of "legitimate interest when processing sensitive data and is forbidden to use sensitive data for marketing purposes.

7.3 PDPL Key Principles

7.3.1 The PDPL contains a number of key principles which apply to the collection and processing of personal data, and which underpin everything that follows:

The Data Subjects Rights	The right to be informed, the right to access their Personal Data, the right to request correction, the right to request the Destruction of their Personal Data, the right to obtain their Personal Data in a legible and clear format. And the right to be immediately informed in case of data breach.
The Data Subject's Consent	Except for the cases stated under the PDPL Law, no Personal Data may be processed, or the purpose of Processing of Personal Data may be changed without the consent of the Personal Data Subject.
Personal Data Disclosure	Personal Data shall not be disclosed to any other party except in cases described in the PDPL and regulations.
Lawfulness, fairness, and transparency	Ensure that it processes and discloses personal data only after having an appropriate lawful basis for such processing. The method by which Personal Data is collected must be direct, clear, and secure, and not entail deception, misleading actions, or blackmail.
Purpose limitation	The Personal Data should only be processed for the purpose for which it was originally collected, subject to the Data Owner's consent to any change to those purposes and separate consent shall be obtained for each new separate processing purpose.
Data minimization	Entity must only collect and process the minimum amount of personal data that is relevant, necessary, and adequate to fulfill the legitimate purposes for which it is processed.
Accuracy	The Controller should not process Personal Data without verifying its accuracy, completeness, timeliness, and relevance for the purpose.
Storage limitation	The Controller shall keep a record of the Personal Data processing activities during the period of the Processing, in addition to at least five years starting from the date of completion of the personal data processing activity.

Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful access, processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
Accountability	The data controller shall be responsible for, and be able to demonstrate compliance with, the PDPL.

8. Key Responsibilities

8.1.1 The Management is ultimately responsible collectively for ensuring that the company meets its legal obligations, and that this policy is followed.

8.1.2 The Management shall issue rules for the appointment of the Data Protection Officer (DPO), which shall include the circumstances under which a data protection officer shall be appointed in compliance with the latest and applicable regulations issued by the Regulatory Authority.

8.1.3 In accordance with the regulations in force, the Management shall appoint the DPO. The Data Protection Officer (DPO) shall be responsible for:

a. Acting as direct point of contact with the regulatory authority and carry out the authority's decisions and instructions in relation to implementing the provisions of the Law and regulations.

b. Keeping the management updated, provide support and advice to help FBSU about personal data protection responsibilities, risks, and issues in line with provisions of the PDPL.

c. Supervise the impact assessment procedures and review audit reports relating to Personal Data protection rules and document the assessment results and issue the recommendations necessary to implement them.

d. Enable the Personal Data subject to exercise their rights under the Law.

e. Respond to the requests made by the Personal Data Subject or their representative and respond to the Regulatory Authority in relation to the complaints made in accordance with the Law.

f. Reviewing and following up personal data of FBSU may process directly or through any third party and review required protection procedures and related policies, in line with an agreed schedule.

g. Deal with violations related to Personal Data and take corrective actions in relation to
   I. Arranging data protection training and advice for everyone to whom this policy applies
   II. Handling data protection queries from staff and contractors.

h. Dealing with requests from anyone whose data we hold for access to that data (known as 'subject access requests').

i. Checking and approving any contracts or agreements with parties that may handle our personal data.

j. Checking and approving any contracts or agreements with parties whose personal data might be handled by FBSU.

k. Ensuring that policies on processing, retention, storage, and deletion of Personal data are adhered to and relevant documentation is maintained to prove compliance.

l. Organize training programs for the employees as necessary to qualify them according to the requirements of the Law.

8.1.4 The IT department is responsible for:

a) Ensuring that all systems, services and equipment used for storing data meet acceptable security standards and PDPL requirements.

b) Performing regular checks to ensure that security hardware and software is functioning properly.

c) Evaluating any third-party services the company is considering using to store or process data in coordination with Legal Department.

d) Implement necessary security and technical measures to limit security risks related to Personal Data Breach.

e) Comply with relevant controls, standards, and rules issued by the National Cybersecurity Authority or recognized best practices and cybersecurity standards if the company is not obligated to follow the controls, standards, and rules issued by the National Cybersecurity Authority.

8.2 Lawful, Fair and Transparent Data Processing

8.2.1 We are responsible as a company for ensuring that any personal data we hold is processed in accordance with the principles laid out as per the PDPL and relevant regulations. We are permitted to process Personal data where one of the following lawful basis applies:

a) The data subject has given their **consent**.

b) The data processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering a contract with them.

c) The processing is necessary for Personal Data controller where the Processing is required pursuant to another law.

d) Processing is necessary to **protect the vital interests of the data subject** or another natural person but communicating with the Personal Data Subject is impossible or difficult.

e) The processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the data controller. This is

usually used by public authorities carrying out vital functions such as provision of public utilities or public safety.

f) The processing is necessary for the purposes of **legitimate** interests pursued by the data controller or by a third party, without prejudice to the rights or interests of the Personal Data Subject, and provided that the Personal Data is not Sensitive Personal Data, in accordance with the rules and provisions set out in the Regulations.

8.2.2 The FBSU will adhere to the following principles:

a) The FBSU collects and processes the personal data that may include:
   I. Personal data obtained directly from data subjects, and
   II. Personal data obtained from third parties.

b) The FBSU only collects, processes, and holds personal data for the specific purposes, or for other purposes expressly permitted by the PDPL.

c) The FBSU shall keep data subjects informed at all times of the purpose(s) for which FBSU processes their personal data.

d) Where personal data will be disclosed to third parties, the FBSU shall only do so where are legally required or permitted.

e) The FBSU shall only collect and process personal data for and to the extent necessary for those specified purpose(s).

f) In respect of personal data that the FBSU shall collect and process, and:
   I. keep it accurate and up to date
   II. Grant the data subject the right to rectify any inaccurate data in accordance with their right to do so
   III. Regularly check the data and ensure that all reasonable steps are taken to promptly rectify or delete any mistakes or inaccuracies as appropriate
   IV. Not keep personal data any longer than is necessary, bearing in mind the purpose(s) for which it was collected
   V. Take all reasonable steps to delete or dispose of any data which is no longer required promptly
   VI. Adhere to the retention policy, which is available to all staff
   VII. Take measures to ensure the security of the data in line with the measures set out law. (Refer data security section)

8.2 Lawful, Fair, and Transparent Data Processing

8.2.1 We are responsible as a university for ensuring that any personal data we hold is processed in accordance with the principles laid out as per the PDPL and relevant regulations. We are permitted to process Personal data where one of the following lawful basis applies:

a) The data subject has given their consent.

b) The data processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering a contract with them.

c) The processing is necessary for Personal Data controller where the Processing is required pursuant to another law.

d) Processing is necessary to protect the vital interests of the data subject or another natural person but communicating with the Personal Data Subject is impossible or difficult.

e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. This is usually used by public authorities carrying out vital functions such as provision of public utilities or public safety.

f) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party, without prejudice to the rights or interests of the Personal Data Subject, and provided that the Personal Data is not Sensitive Personal Data, in accordance with the rules and provisions set out in the Regulations.

8.3 Consent Requirements

8.3.1 If the Personal Data is collected directly from the Data Subject, the FBSU shall, before or when collecting the data shall make following necessary measures to inform the Data Subject of the following:

a) FBSU's identity, its contact details, and any other details related to the channels established by the university for the purpose of communicating in relation with Personal Data protection.

b) Contact details of the data protection officer appointed by the Controller, where applicable.

c) The legal basis and a specific, clear, and explicit purpose for collecting and Processing Personal Data.

d) The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.

e) Explanation about Data Subject rights and mechanisms for exercising those rights.

f) Explanation on how to withdraw consent given to process of any Personal Data.

g) Explaining whether collecting or processing personal data is mandatory or optional.

8.3.2 FBSU shall not process personal data without the consent of its owner except for the cases stipulated below i.e. consent is not required for the following:

a) If the processing would achieve a clear benefit and it is impossible or impractical to contact the data subject or communicating with the Personal Data Subject is impossible or difficult.

b) If it is required by law or prior agreement to which the data subject is a party.

c) If the controller is a public entity and the processing is required for security or judicial purposes.

d) If the processing is necessary to achieve a lawful interest of the controller or any other party, without prejudice to the rights and interests of the Personal Data subject and provided that the Personal Data is not Sensitive Personal Data, in accordance with the rules and provisions set out in KSA regulations.

8.4 Consent Requirements – For Scientific, Research or Statistical Purposes

8.4.1 Personal data may be collected or processed for scientific, research or statistical purposes without the consent of its owner (the Data Subject) in the following cases:

a) The Company clearly and accurately specifies the scientific, research, or statistical purposes in the records of Personal Data Processing Activities.

b) The FBSU takes the necessary measures to ensure that only the minimal Personal Data necessary to achieve the specified purposes is collected.

c) The FBSU shall Pseudonymize Personal Data that is being processed, in cases where this does not impact the achievement of the Processing Purpose.

d) The FBSU shall take necessary measures to ensure that the Processing does not have any negative impact on the rights and interests of the Data subject.

8.4.2 The FBSU shall observe the following when collecting or processing personal data for scientific, research or statistical purposes without consent:

a) Identify the scientific, research or statistical purposes clearly and accurately.

b) Document the procedures of identifying the data content according to the specific purposes, including, without limitation, by using data charts that show the need for each piece of data and linking it to each of the objectives of the study.

c) The data to be collected or processed shall not include anything that specifically indicates the identity of the Data Subjects.

d) Assess the potential risks and adverse effects that may result from processing such data, including the risks relating to the possibility of identifying the Data Subjects specifically.

8.5 Personal Data Collection

8.5.1 The FBSU should collect Personal Data directly from the relevant Data Owner. However, the university may only collect Personal Data from a person other than the Data Owner in the following circumstances:

a) The Personal Data Owner agrees to such collection.

b) The Personal Data is publicly available or collected from a publicly available source.

c) The Company is a government entity, and such collection is for security purposes or to satisfy judicial requirements.

d) The Data Owner's vital interests would be harmed if their Personal Data is not collected from such other person.

e) The collection of Personal Data is necessary to protect public health or safety, or to protect the life or health of a specific individual.

f) If the Personal Data will not be recorded or stored in a form that makes it possible to directly or indirectly identify the Personal Data Subject.

g) The Regulations set out the rules and procedures applicable in this regard if the Collection or Processing of the Personal Data is necessary to achieve lawful interests of the Controller or any other party, without prejudice to the rights or interests of the Personal Data Subject, and provided that the Personal Data is not Sensitive Personal Data, in accordance with the rules and provisions set out in the Regulations.

h) If Personal Data is collected from a party other than the Data Subject, the FBSU shall, without undue delay and within a period not exceeding (30) days, take necessary steps to provide to the Data Subject information, in addition to the categories of Personal Data being processed and the source from which the Controller obtained it. This requirement shall not
   I. apply in any of the following conditions if:
   II. The information is already available to the Data Subject.
   III. The provision of such information proves impossible or would involve a disproportionate effort.
   IV. The FBSU collects data to fulfil a legal requirement.
   V. The FBSU is a Public Entity, and the Collection of Personal Data is for security purposes, or to fulfil judicial requirements, or to achieve a Public Interest.
   VI. Personal Data is subject to an obligation to professional secrecy regulated by a law.

8.6 Personal Data Retention and Record of Data Processing

8.6.1 The FBSU shall, without undue delay, destroy the Personal Data when no longer necessary for the purpose for which they were collected. However, the university may retain data after the purpose of the Collection ceases to exist; provided that it does not contain anything that may lead to specifically identifying the Data Subject in line with the controls stipulated in the Regulations.

8.6.2 In the following cases, the FBSU shall retain the Personal Data after the purpose of the Collection ceases to exist:

a) If there is a legal basis for retaining Personal Data for a specific period, in which case the Personal Data shall be destroyed upon the lapse of that period or when the purpose of the Collection is satisfied, whichever longer.

b) If the Personal Data is closely related to a case under consideration before a judicial authority and the retention of the Personal Data is required for that purpose, in which case the Personal Data shall be destroyed once the judicial procedures are concluded.

8.6.3 FBSU shall keep records of their processing activities for a period determined by relevant regulations. The records should include a minimum of the following data:

a) University name (FBSU) and relevant contact details.

b) Information about the Data Protection Officer, where required in accordance with regulation.

c) Purposes of Personal Data processing.

d) Description of Personal Data categories being processed and Data Subjects categories.

e) Retention periods for each Personal Data category, where possible.

f) Categories of recipients to whom the Personal Data is disclosed.

g) Description of operations of Personal Data Transfer outside the Kingdom, including the legal basis for the Transfer and recipient parties.

h) Description of the procedures and organizational, administrative, and technical measures in place that ensure the security of Personal Data, where possible.

8.6.4 FBSU shall provide access to the records of Personal Data Processing activities to the Regulatory Authority upon request.

8.7 Processor Selection

8.7.1 The FBSU shall ensure that any Data Processor selected provides sufficient guarantees to protect Personal Data, and that the agreement with the Processor includes the following:

a) Purpose of the Processing.

b) Categories of Personal Data being processed.

c) Duration of the Processing.

d) Processor's commitment to notify, without undue delay, the university in case a Personal Data Breach occurs, in accordance with the provisions of the PDPL and Regulation.

e) Clarification of whether the Processor is subject to Regulations in other countries and the impact on their compliance with the Law and its Regulations.

f) Not requiring the Data Subject's prior consent for mandatory Disclosure of Personal Data under the applicable laws in the Kingdom, provided that the Processor notifies the FBSU of such Disclosure.

g) Identifying any subcontractors contracted by the Processor, or any other party to whom Personal Data will be disclosed.

8.7.2 The FBSU shall issue clear instructions to the Processor, and in case of any violation of the university's instructions or any applicable laws in the Kingdom, the Processor shall notify the FBSU in writing without undue delay.

8.7.3 The FBSU is responsible to periodically assess Processor's compliance with the Law and its Regulations, and ensuring that all regulatory requirements are met, whether the Processing is achieved by the Processor or third parties acting under their behalf. The FBSU may appoint an independent third party to assess and monitor Processor's compliance on its behalf.

8.7.4 If Processor violates the instructions issued by the FBSU or the agreement regarding the Processing of Personal Data, the Processor shall be considered as a Company and held directly accountable for any violation of any provisions of the Law.

8.7.5 Before entering any subsequent contracts with Sub-Processors, the Processor shall abide by the following:

a) Take sufficient guarantees to ensure that such contracts would not impact the level of protection provided to the Personal Data being processed.

b) Choose only sub-Processors that provide the sufficient guarantees to comply with the Law and its Regulations.

c) Obtain prior acceptance from Company, with the Controller being notified before entering into such contracts and enabling the Controller to object to them within a timeframe agreed upon between the Controller and the Processor.

8.8 Disclosure of Personal Data

8.8.1 The FBSU may only disclose personal data to third parties in the following cases:

a) If the personal data subject consents to the disclosure in accordance with the provisions of the law.

b) If the personal data is collected from a publicly available source, under the condition that such data have not been made available to the public in violation of the provisions of the Law and its Regulations.

c) If the entity requesting the disclosure is a Public Entity and the request is made for security purposes, to implement another law, or to fulfill judicial requirements. The Disclosure is necessary to protect public health, public safety, or to protect the lives or health of specific individuals.

d) The Disclosure will only involve subsequent Processing in a form that makes it impossible to directly or indirectly identify the Data Subject.

e) The Disclosure is necessary to achieve legitimate interests of the FBSU, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed.

f) When disclosing Personal Data in response to a request from a public authority for security purposes, or to fulfil requirements of another law, or to fulfil judicial requirements, or if the disclosure is necessary to protect public health or public safety, or to protect the life of specific individuals' or their health, the following measures shall be taken:
   I. Document the request for Disclosure.
   II. Accurately identify the type of Personal Data required to be disclosed.

8.8.2 The FBSU shall not disclose Personal Data if the Disclosure:

a) Represents a threat to security, harms the reputation of the Kingdom, or conflicts with the interests of the Kingdom.

b) Affects the Kingdom's relations with any other state.

c) Prevents the detection of a crime, affects the rights of an accused to a fair trial, or affects the integrity of existing criminal procedures.

d) Compromises the safety of an individual.

e) Results in violating the privacy of an individual other than the Data Subject, as set out in the Regulations.

f) Conflicts with the interests of a person that fully or partially lacks legal capacity.

g) Violates legally established professional obligations.

h) Involves a violation of an obligation, procedure, or judicial decision.

i) Exposes the identity of a confidential source of information in a manner detrimental to the public interest.

8.8.3 Except for disclosure requested by Public entity or is necessary to protect public health, the FBSU shall consider the following when disclosing Personal Data:

a) Disclosure request is closely related to a specific and clear purpose or subject.

b) Necessary care shall be provided to protect the privacy of the Data Subject or any other individual.

c) Disclosure is limited to the minimum amount of Personal Data necessary to achieve the purpose.

8.8.4 The FBSU shall keep up to date records of all disclosures. Such records shall include the dates, methods, and purposes of the disclosure.

8.8.5 Except for disclosure requested by Public entity or is necessary to protect public health, when disclosing Personal Data related to another person who is not the Data Subject, the Company shall take necessary care and provide sufficient guarantees to ensure the privacy of the other individual is preserved and not violated. This includes considering the following steps:

a) In each separate case, balancing between the rights of the Data Subject and the rights of the other person.

b) Whenever possible, pseudonymization of Personal Data allowing the identification of the other person.

8.8.6 Data subjects have a right to request that the FBSU ceases to disclose any personal data that is held about them. Management is required to ensure that all data subjects are appropriately informed about these rights and establish dedicated channels for data subjects to exercise these rights.

8.8.7 If Personal Data is corrected, completed, or updated, the FBSU shall notify such amendment to all the other entities to which such Personal Data has been transferred and make the amendment available to such entities.

8.9 Restriction of Personal Data

8.9.1 The law stipulates certain conditions where the FBSU may put restrictions over personal data disclosing.

a) Except for reasons decided by law, The FBSU shall not disclose personal data in the following cases.

b) It represents a threat to security, harms the reputation of the Kingdom, or conflicts with the interests of the Kingdom.

c) It affects the Kingdom's relations with any other state.

d) It prevents the detection of a crime, affects the rights of an accused to a fair trial, or affects the integrity of existing criminal procedures.

e) It results in violating the privacy of an individual other than the personal data subject, within the regulations requirements.

f) It conflicts with the interests of a person that fully or partially lacks legal capacity.

g) It breaches legally established professional obligations.

h) It involves a breach of an obligation, procedure, or judicial ruling.

i) It exposes the identity of a confidential source of information in a manner detrimental to the public interest.

8.10 Communication, Duration and Documentation Data Subjects Requests

a) The FBSU may apply the appropriate procedures and means to communicate with Personal Data Subjects and provide them with the necessary information in a concise, clear and easily accessible manner, and use clear and express language that suits the target category, taking into account the law and regulation.

b) The FBSU shall, upon receiving a request from the Data Subject regarding their rights as stipulated in the Law carry out the request for Personal Data Subject within 30 days of receiving the request. If carrying out the request requires extraordinary

efforts or if the company receives multiple requests from the same Personal Data Subject, the company may extend the more than 30 additional days, provided the company shall notify the Personal Data Subject of such extension and the justifications therefor.

c) The FBSU shall take the necessary technical, administrative, and organizational measures to ensure a prompt response to requests related to exercising rights.

d) The FBSU shall take appropriate measures to verify the identity of the requester before executing the request in accordance with relevant legal requirements.

e) The company shall document and keep the details of the requests it receives, including any verbal request.

f) The FBSU may refuse to act on request when it is repetitive, manifestly unfounded, or requires disproportionate efforts, in which the Data Subject shall be notified of such reason.

8.11 Data Impact Assessment

8.11.1 The Part of the FBSU's duty is to ensure that in the planning of new processes or procedures which involve the use of personal data provided to the public which may adversely affect the privacy of Personal Data Subjects. The university will always ensure that all such changes are designed and implemented in accordance with the regulation, and that the DPO is consulted, and their recommendations are considered in the planning and introduction of such changes.

8.11.2 In any situation where the processing of the personal data is likely to result in a high risk to the data subjects' rights and freedoms under the law, a data impact assessment is required to be carried out, overseen by the DPO. The data processor, if any, shall be provided with a copy of a form prepared by the controller for the purpose of impact assessment.

8.11.3 The impact assessment form shall:

a) Purpose of the processing and its legal basis.

b) Describe the nature of the processing by clarifying the processing activities to be carried out, the type and source of the Personal Data, and the parties with which the personal Data is to be shared or disclosed.

c) Describe the scope of the processing by identifying the type of personal data and the geographical scope of the processing.

d) Describe the context of the processing by identifying the relation between the Personal Data Subject, the Controller (the company), and the Processors, and all the other relevant circumstances.

e) Assess the necessity and proportionality by identifying means that enable the entity to use the minimum amount of data required to fulfill the purpose of the processing.

f) Identify the legal justification and practical Need of the processing.

g) Identify and assess risks of the data processing based on their severity of its impact, materially and morally, and the likelihood of any negative impact on Data Subjects, including any psychological, social, physical, or financial impact and likelihood of their occurrence.

h) Identify measures and solutions to mitigate risks.

i) Review the results of the risks and the appropriateness of the measures taken in respect of such risks.

8.11.4 Further, the FBSU shall conduct impact and risks assessment in each of the following cases:

a) Collection and processing of Sensitive Data including collecting, comparing, or linking two or more sets of Personal Data obtained from different sources.

b) The activity of company includes: continuous and large scale Processing of Personal Data of those who fully or partially lack legal capacity, or Processing operations that by their nature require continuous monitoring of Data Subjects, or Processing Personal Data using new technologies, or making decisions based on automated Processing of Personal Data.

c) Providing a product or service that involves Processing Personal Data that is likely to cause serious harm to the privacy of Data subjects.

8.11.5 The FBSU shall provide a copy of the impact assessment to any Processor acting on its behalf in relation to the relevant Processing.

8.11.6 In the event where Data Processing operation will harm the privacy of the Data Subjects, FBSU shall address the reasons for that and re-conduct the assessment.

8.11.7 In the event of high risks or unavailability of means to apply the solutions stated in the impact assessment form to reduce those risks, the FBSU may report that to the Regulatory Authority to consider whether it is possible to take other measures that reduce the risks and are in line with the capability of the university.

8.12 Providing Information to Data Subjects

8.12.1 Management is required to ensure that, when collecting and processing personal data, the data subject is aware of the purposes for which this is being done, and what is happening to the data. Management should ensure that the following principles are followed:

a) Where we collect personal data directly from the data subject, we will inform them of the purpose for which it is being collected at the time of collection.

b) Where we are obtaining personal data from a third party, the data subject needs to be

c) All data subjects will be provided with the following information:

- Details of the FBSU, including the name of the DPO
- Why the data is being collected and processed, and the legal basis for this

- If applicable, any legitimate interests justifying the Company's collection and processing of data where the data is to be transferred to third party/parties, their details
- Where data is to be transferred outside KSA, details of the transfer including the:
  - Approval from data regulator
  - Details of data retention
  - Details of the data subject's rights under PDPL
  - The Data Subject Right to withdraw consent to processing at any time
- Details of any legal or contractual requirement which means that the company needs to collect this information and process it, and what the implications are if it cannot do so.

8.12.2 The FBSU shall adopt a privacy policy and make it available to Personal Data Subject for review prior to collecting Personal Data. The policy shall specify the purpose of Collection, the Personal Data to be collected, the method of Collection, the means of storage and Processing, the manner in which the Personal Data shall be destroyed, and the rights of the Personal Data Subject in relation to the Personal Data and how such rights shall be exercised.

8.13 Data Subject Access

8.13.1 Data subjects have the right to access their personal data from the organization or obtain copy of it in a clear and readable format, in conformity with the content of the records, at no cost.

8.13.2 The FBSU shall enable Personal Data Subject to access their Personal Data or obtain a copy thereof, subject to the following:

a) Verify the identity of the Personal Data Subject or their representative before enabling them to access their data or obtain a copy thereof.

b) The foregoing shall be conducted in a secure, easy and clear manner, and shall include all the data which the FBSU keeps concerning the Personal Data Subject as has been collected directly from the Personal Data Subject.

c) Not disclose any Personal Data that identifies any other person. Where that is not possible, the consent of the other person shall be obtained.

8.13.3 Subject Access Requests (SARS) can be made by data subjects where an organization holds personal data about them. The requests are made in order for the data subject to find out what data is being held, and what is being done with it.

8.13.4 SARs need to be made by the data subject.

a) They should be addressed to the DPO, who will deal with the request.

b) The FBSU will usually respond to them within 30 days.

8.13.5 The FBSU may restrict the said right of data subject access in the following cases:

a) If this is necessary to protect the personal data subject or others from any harm, as set out in the Regulations.

b) If the company is a public entity and the restriction is required for security purposes to implement another law, or to fulfill judicial requirements.

c) If it represents a threat to security, harms the reputation of Kingdom, or conflicts with the interests of the Kingdom.

d) Affects the Kingdom's relations with any other state.

e) Prevents the detection of a crime, affects the rights of an accused to a fair trial, or affects the integrity of existing criminal procedures.

f) Compromise the safety of an individual.

g) Results in violating the privacy of an individual other than the Personal Data Subject, as set out in the Regulations.

h) Conflicts with the interests of a person that fully or partially lacks legal capacity.

8.14 Rectification of Personal Data

8.14.1 Data subject shall have the right to rectify, supplement or update their Personal Data held by the company and the company must notify any party to whom the Personal Data has been transferred of the rectification.

8.14.2 Where a data subject informs management that data which is held about them is inaccurate or incomplete and requests that it is corrected, management will rectify the information and inform the data subject once it is completed, within 30 days of the request.

8.14.3 Where the incorrect data is held by third parties to whom it has been disclosed, management shall ensure that they are informed and that the data that they hold is rectified.

8.14.4 When correcting or completing Personal Data, or updating Personal Data at the request of Personal Data Subject, the company shall:

a) Verify the identity of the Personal Data Subject or their representative.

b) Apply measures sufficient to ensure accuracy and integrity of the data, by examining and auditing the documents and evidence accompanying the correction request. That shall not apply to data representing the opinion of the Personal Data Subject.

c) Set such measures as necessary to notify other entities, which the said data has been shared with, and request that the processing of such data be restricted until the correction request is completed and notify the Personal Data subject accordingly.

d) Notify the Personal Data Subject upon the correction, completion or updating of their data, and lift the restrictions imposed on processing.

e) Notify the Personal Data Subject in the event that their request is rejected, provided the rejection shall be justified, and inform the Personal Data Subject of their right to make a complaint.

f) Document all the updates made to Personal Data.

8.15 Erasure of Personal Data

8.15.1 Data subjects have a right to require the FBSU to erase personal data held about them through a formal documented request when

a) The FBSU no longer needs the data it is holding for the purposes for which it was originally collected

b) The data subject wishes to withdraw their consent to the company holding and processing the data

c) The data subject objects to the company holding and processing the data, and there is no overriding legitimate interest which allows management to continue to do so

d) The personal data has been processed unlawfully

e) The personal data needs to be erased in order for the FBSU to comply with a particular legal obligation

f) Direct marketing is the purpose for which the data erasure request is processed.

8.15.2 When destroying the Personal Data, the FBSU shall:

a) Verify the identity of the Personal Data Subject before destroying their data.

b) Exercise due care and give priority to destruction requests relating to those fully or partially legally incompetent.

c) Set such measures as necessary to notify other entities with which the data has been shared and request the destruction of such data, and notify the Personal Data subject accordingly.

d) Establish the necessary procedures and sufficient steps as practicably possible to notify the other entities whose available means have been used to publish the Personal Data, including what has been published on social media.

e) Destroy all the Personal Data copies stored with the company, whether archived data or backup copies, in accordance with the timeline and procedures set by the company.

8.15.3 Where management is obliged, it will erase the information and inform the data subject that it has been completed, within 30 days of the request. In complex cases, it may be extended by up to 30 days, and where the data is held by third parties to whom it has been disclosed, management has to ensure that they are informed and that the data that they hold is erased.

8.15.4 However, subject to the FBSU's ability to anonymize it to prevent identification of the Data Owner and subject to any legal justification or court proceedings that mean that it needs to be retained.

8.15.5 The controller shall destroy the personal data as soon as the purpose of its collection ends. However, it may keep such data after the purpose of its collection has ended, if everything that leads to specifically knowing its owner is removed in accordance with the controls specified by the regulations.

8.15.6 The controller shall keep the personal data even after the purpose of its collection has ended or even the data subject has requested for destruction of the data in the following two cases:

a) If there is a legal justification that requires keeping it for a specific period, and in this case it shall be destroyed after the expiry of this period or the purpose of its collection, whichever is longer.

b) If the personal data is closely related to a case under consideration before a judicial authority and its retention is required for this purpose, and in this case, it shall be destroyed after completing the judicial procedures related to the case.

8.16 Objections to Personal Data Processing

8.16.1 Data subjects have a right to object to further processing their personal data. Where the data subject notifies of their objection, management will cease such processing immediately unless legitimate interests override those of the data subject, or unless management needs to continue to process the data in conducting a legal claim.

8.17 Data storage and General Security

8.17.1 The FBSU shall apply such organizational, administrative, and technological means and measures to confirm privacy of Personal Data Subjects at all the stages where their Personal Data is dealt with, used and transferred.

8.17.2 That shall include the following:

a) Assess the potential risks and adverse effects of processing Personal Data and set and apply such controls and procedures as necessary to avoid or, at least, mitigate such risks.

b) Adhere to all controls, standards, guidelines, and other provisions issued by the National Cybersecurity Authority. If the Company is located outside the Kingdom, the Company shall adopt the international best practices and the best standards widely in use in relation to cybersecurity.

c) All electronic copies of personal data should be stored securely using privilege levels and passwords.

d) Regular password changes will be enforced, and the number of logins will be restricted.

e) Passwords should never be written down or shared between any employees, agents, contractors or other persons working on behalf of the Company, no matter what their level of seniority.

f) Computer equipment belonging to the FBSU will be sited in a secure location within the office and in a position where they cannot be viewed by members of the public

g) Computer terminals must not be left unattended, and should be logged off at the end of the session.

h) Personal data to be backed up and stored and, where appropriate, are encrypted.

I All software must be kept up to date and shall be responsible for ensuring that all security- related updates are installed promptly, unless there are valid technical reasons for not doing so.

j) No software should be installed on the university's system without the prior approval of IT Director at FBSU.

k) Personal data should not be stored on any mobile device such as laptops, tablets and smartphones without the approval of the DPO and, where it is held, only in accordance with their instructions and limitations.

l) Personal data must never be transferred onto an employee's personal device and the Company shall ensure that such data is never transferred onto a device owned by a contractor or agent unless they have agreed to comply fully with the letter and spirit of this policy and with the PDPL.

m) All manual files must be stored securely in locked cabinets and should not be left unsecured in the office overnight.

n) Computer printouts containing personal information should be destroyed without delay and should never be retained for scrap paper.

o) Where personal data is to be erased, or otherwise disposed of, this will be done in accordance with the FBSU's data retention policy.

8.18 Access to Personal Data

8.18.1 In relation to accessing personal data:

a) Employees must never access data either on a computer or in paper form, without having authority to do so.

b) Personal data must not be shared informally and if an employee, agent, contractor, or any other third party wants access to the data, it must be formally requested from the DPO.

c) Personal data must be handled with care and should not be left unattended or in view of unauthorized employees, contractors or agents, whether on paper or on a screen.

8.19 Organizational Measures

8.19.1 The FBSU shall take the following steps in relation to the collection, holding and processing of personal data:

a) All employees, agents, contactors, or other parties working on our behalf and might have access to any Personal Data will be made fully aware of their individual responsibilities, and the responsibilities of the company, in relation to data privacy and the PDPL, and they will be provided with a copy of this policy.

b) In respect of these individuals and of personal data held by the company

- Only those persons who need access to personal data in order to complete their assigned duties will be granted such access. Such persons will be appropriately trained and supervised in handling personal data.
- Such persons will be encouraged to exercise caution in discussing work-related matters within the workplace.
- All employees are bound by strict duties of professional confidentiality in discussing any work- related matters outside the workplace, which will be adhered to and enforced.

c) All The methods of collecting, holding and processing data shall be regularly evaluated and reviewed. The personal data held by the company shall be reviewed periodically, as set out in data retention policy.

d) The FBSU shall keep the performance of its agents, contractors and third parties under review; and ensure that they are required to handle personal data in accordance with the PDPL and our policy. The company shall also ensure that they are held to the same standards as its own employees, both contractually and in practice.

e) Where any agent, contractor or third party fails in their obligations under this policy, the FBSU shall ensure that they are required to indemnify us for costs, losses, damages, or claims which may arise as a result.

8.20 Dealing with Health Data

8.20.1 The FBSU shall apply such organizational, technological, technical, and administrative means and measures as sufficient to protect Health Data from any unauthorized use, misuse, use for any purpose other than that for which the data has been collected, breach or destruction, and shall apply any means and measures that ensure confidentiality of Health Data.

8.20.2 The FBSU shall apply following controls and measures:

a) Prevent access by any entity or individual to such data, other than those who are assigned specifically by the management.

b) Limit the processing of Health Data, to the extent possible, to the minimum number of employees, who shall be honest and responsible, while identifying their roles and the

limits of their duties and having them sign an agreement to maintain the confidentiality of, and not disclose, such data.

c) State in the contracts entered into between the FBSU and Data Processors for carrying out of work or tasks related to processing of Health Data, provisions that obligate them to follow the foregoing means and measures.

d) Document all stages of Health Data Processing and provide the means to identify the person in charge of each stage.

E Incorporate into the FBSU codes of conduct the general rules contained in the Law and regulations.

f) Adapt and implement applicable regulatory requirements and controls issued by the Ministry of Health, the Saudi Central Bank and the Saudi Health Council in coordination with the Council of Health Insurance and related entities regarding management of health data.

8.21 Transfer of Personal Data Outside KSA

8.21.1 Under certain conditions, FBSU may Transfer Personal Data or disclose it to a party outside the Kingdom, provided that such Transfer or Disclosure does not impact national security or vital Interests of the Kingdom or violate any other law in the Kingdom.

8.21.2 Controller may Transfer Personal Data outside the Kingdom or disclose it to a party outside the Kingdom, to achieve any of the following purposes:

a) If this is relating to performing an obligation under an agreement to which the Kingdom is a party.

b) If it is to serve the interests of the Kingdom.

c) If this is to the performance of an obligation to which the Data Subject is a party

d) If conducting processing operations enables the Controller to carry out its activities, including central management operations.

e) If that results in providing a service or benefit to the personal data subject.

f) If this is to conduct scientific research and studies

8.22 Personal Data Transfer Conditions

8.22.1 The conditions that must be met when there is a Transfer or Disclosure of Personal Data outside Kingdom, are as follows:

a) The Transfer or Disclosure shall not cause any prejudice to national security or the vital interests of the Kingdom.

b) There is an adequate level of protection for Personal Data outside the Kingdom. Such level of protection shall be at least equivalent to the level of protection guaranteed by the Law and Regulations, according to the results of an assessment conducted by the

Regulatory Authority in coordination with whomever it deems appropriate from the other relevant authorities.

c) The Transfer or Disclosure shall be limited to the minimum amount of Personal Data needed.

d) The Company shall limit the Transfer or Disclosure of Personal Data outside the Kingdom to a party outside the Kingdom to the minimum necessary to achieve the purpose of the Transfer or Disclosure through the use of any appropriate mean including data maps that indicate the need to Transfer or disclose each data and link it to one of the purposes for processing outside the Kingdom.

e) When transferring or disclosing Personal Data to a party outside the Kingdom, the FBSU shall ensure that such Transfer or Disclosure does not impact the privacy of Data Subjects or the level of protection guaranteed for Personal Data under the Law and its Regulations, by ensuring that the Transfer or Disclosure will not compromise - at least- any of the following:

I. Data Subject's ability to exercise their rights guaranteed by the Law.
II. Data Subject's ability to withdraw their consent to the processing.
III. Company's ability to comply with requirements for notifying Personal Data Breaches.
IV. Company's ability to comply with provisions, controls, and procedures for disclosing Personal Data.
V. Company's ability to comply with provisions and controls for destroying Personal Data.
VI. Company's ability to take necessary organizational, administrative, and technical measures to ensure the security of Personal Data.

8.22.2 If any of the control breach is identified, the FBSU must do the following:

a) Stop – without undue delay – the process of transferring personal data outside the Kingdom or disclosing it to a party outside the Kingdom.

b) Re-assess the risks of transferring personal data outside the Kingdom or disclosing it to a party outside the Kingdom.

8.22.3 The above conditions shall not apply to cases of extreme necessity to preserve the life or vital Interests of the Data Subject or to prevent, examine or treat disease.

8.23 Risk Assessment of Transferring or Disclosing Personal Data Outside KSA

8.23.1 The FBSU shall conduct a risk assessment of the Transfer of Personal Data outside the Kingdom or Disclosure to a party outside the Kingdom in any of the following cases:

a) Transform data outside the Kingdom in accordance with transfer based on appropriate safeguards of transferring Personal Data outside KSA.

b) Transfer of data outside the Kingdom in accordance with cases where the appropriate safeguards of Personal Data outside KSA are not required.

c) Continuous or large-scale Transfer of Sensitive Data outside the Kingdom.

8.23.2 The FBSU shall conduct a risk assessment of the Transfer of Personal Data outside the Kingdom or Disclosure to a party outside the Kingdom in any of the following cases:

a) The purpose of the Transfer or Disclosure and its legal basis.

b) Description of the nature of the Transfer or Disclosure to be carried out and its geographic scope.

c) Means and appropriate safeguards adopted for the Transfer of Personal Data outside the Kingdom and the extent to which they are sufficient to achieve the required level of protection for Personal Data.

d) Measures taken to ensure that the Transfer or Disclosure is limited to the minimum amount of Personal Data necessary to achieve the purposes.

e) The material or moral impact that may result from the Transfer or Disclosure, and the possibility of any harm to Data Subjects.

f) Measures to prevent and mitigate identified risks to protect Personal Data.

8.24 Data Breach Notification

8.24.1 All personal data breaches including data leakage, damaged, unauthorized, or illegally accessed must be reported immediately to the DPO.

8.24.2 If such a breach occurs, and it is likely to result in a risk to the rights and freedoms of data subjects e.g. financial loss, breach of confidentiality, reputational damage the DPO is required to ensure that it is informed without delay and, in any event, within 72 hours of the breach to the regulatory authority.

8.24.3 Such notification shall be accompanied by a report that includes the following:

a) Transform an analysis of the Personal Data Breach incident, explaining the incident and the time it occurred, how it occurred and how it has been detected.

b) The categories and number of the affected Personal Data Subjects, and the number of the affected records that contain Personal Data.

c) A description of the actual or potential risks resulting from the incident, including the impact level of it, the pre-adopted measures to prevent such risks, the corrective actions and the steps that have been taken to mitigate the adverse effects of such risks, and the steps that will be taken to avoid recurrence of the incident.

d) Whether the Data Subject has been notified of the Personal Data Breach.

e) Whether the Personal Data Subject or any other party has reported the incident before it occurred, and the entities to which the incident was so reported, if possible.

f) Contact details, including the details of the FBSU, and the contact details of the Personal Data protection officer, if any, or of any other official that has information concerning the incident.

8.24.4 The FBSU shall keep a copy of the reports submitted to the Regulatory Authority and document the corrective measures taken in relation with the Personal Data Breach, as well as any relevant documents or supporting evidence.

8.25 Notifying the Personal Data Subject of Data Breach

8.25.1 Without any undue delay, the FBSU shall notify the Data Subject of a Personal Data Breach, if it may cause damage to their data or conflict with their rights or interests, provided that the notification is in simple and clear language. The following information must be provided:

a) Description of the Personal Data Breach.

b) Description of the potential risks arising from Personal Data Breach, and the measures taken to prevent or limit those risks and limit their impact.

c) The name and contact details of the personal data protection officer, if any, or of any other official, or details of any other manner of communication to obtain more information.

d) Any recommendations and advice to help the Data Subject take appropriate action to avoid potential risks or mitigate their adverse effects.