The Implementing Regulation of the Personal Data Protection Law

Article 1: Definitions

The terms and phrases used in this Regulation shall have the meanings assigned to them in Article (1) of the Personal Data Protection Law issued by Royal Decree No. (M/19) dated 9/2/1443H and amended by Royal Decree No. (M/148) dated 5/9/1444 AH. The following terms and phrases, wherever used in this Regulation, shall have the meanings assigned to them, unless the context requires otherwise:

1- **Regulation:** The Implementing Regulation of the Law.

2- **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 even if this does not include marketing for the sale of a product or service.

3- **Personal Data Breach:** Any incident that leads to unauthorized Disclosure, Destruction, or access to Personal Data, whether intentional or accidental, and by any means, whether automated or manual.

4- **Vital Interest:** Any interest necessary to preserve the life of a Data Subject or any other individual.

5- **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.

6- **Legitimate interest**: refers to any necessary interest of the controller that requires the processing of personal data for a specific purpose.

7- Pseudonymisation: 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.

8- **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.

9- **Secondary Use:** Processing Personal Data for purposes other than the purposes for which it was initially collected.

10- **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.

Article 2: Personal or Family Use

1- The provisions of the Law and the Regulation shall not apply to an individual processing Personal Data for purposes that do not exceed personal or family use.

2- Personal or family use, as referred to in Article 2 of the Law, means that an individual processing Personal Data within their family or limited social circle as part of any social or family activity.

3- The following shall not be considered personal or family use:

a) An individual publishing Personal Data to the public or disclosing it to any person outside the scope specified in paragraph (2) of this article.

b) Using Personal Data for professional, commercial, or non-profit purposes.

Article 3: Legal Basis for Processing Personal Data

The following shall be considered a legal basis for processing or disclosing Personal Data in accordance with Articles (6), (10), and (15) of the Law:

1- The consent of the Data Subject

2- Protecting the Vital Interests of the Data Subject or protecting them from any harm.

3- If the Controller is a Public Entity, and the processing is required by another Law, or for security purposes, or to fulfil judicial requirements, or to achieve a public interest.

4- Protecting public health or safety or protecting a specific individual or individuals or their health.

5- Pursuing a legitimate interest of the Controller or a legitimate interest of the Data Subject.

6- Processing is required under another Law.

7- Executing an agreement in which the Data Subject is a party.

8- If the Personal Data is publicly available or collected from a publicly available source.

Article 4: General Provisions of Data Subject Rights

1- If consent, legitimate interest, or executing an agreement in which the Data Subject is a party is the legal basis for processing Personal Data, the Controller shall, upon receiving a request from the Data Subject regarding their rights as stipulated in the Law, do the following:

a) Act on the request of the data subject for exercising their rights under the Law within a delay not exceeding (30) business days.

b) Extend the period of executing the right to request Destruction or the right to access Personal Data if the execution requires unexpected or unusual effort or if

the Controller receives a significant number of requests from the Data Subject, provided that the Data Subject is notified in advance of the extension with the reasons for the delay.

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

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

e) Take the necessary measures to document and keep record of all submitted, including oral requests.

2- The Controller 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.

3- In cases where the Data Subject fully or partially lacks legal capacity, their legal guardian shall exercise their rights on their behalf.

Article 5: Right to be Informed

1- Without prejudice to the provisions of Articles (6), (10) and (15) of the Law, if the Personal Data is collected directly from the Data Subject, the Controller shall, before or when collecting the Personal Data, take the necessary measures to inform the Data Subject of the following:

a) Controller's identity, its contact details, and any other details related to the channels established by the controller 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.

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's rights, as stipulated in Article (4) of the Law and the 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.

2- When a Controller whose activities require systematic and a large scale processing of Personal Data on individuals that fully or partially lack legal capacity, or continuous monitoring of Data Subjects, adoption of new technologies, or making automated decisions based on Personal Data, shall take the necessary measures to inform the Data Subject of what is stipulated in paragraph (1) of this Article, in addition to the following:

a) Means and methods of collecting and processing Sensitive Data, where applicable.

b) Means and procedures taken to protect Personal Data.

c) Indicate whether decisions will be made based on automated processing of Personal Data.

3- When the Controller engages in additional processing of Personal Data for the purposes of Secondary Use of data, it shall provide the Data Subject with the necessary information in accordance with the provisions of paragraphs (1) or (2) of this Article, as appropriate, before conducting the additional processing.

4- The Controller shall provide the required information in an appropriate language as stipulated in paragraphs (1) and (2) of this Article when aware that the Data Subject fully or partially lacks legal capacity.

5- The provisions of paragraphs (1) and (2) of this Article do not apply in the following cases:

a) If the relevant information is already available to the Data Subject.

b) If providing that information impossible or requires disproportionate efforts.

c) If providing that information conflicts with the prevailing laws in the Kingdom.

Article 6: Right of Access to Personal Data

1- Without prejudice to the provisions of Articles (9) and (16) of the Law, the Data Subject has the right to access their Personal Data available with the Controller, subject to the following:

a) The legal basis for processing is consent, legitimate interest of the Controller, or an agreement to which the Data Subject is a party.

b) Providing access to personal data at a request from the data subject, or via a channel provided by the controller enabling data subject to directly access their personal data without need to make a request.

2- When enabling the Data Subject to access their Personal Data, the Controller shall ensure that it does not involve disclosing Personal Data that identifies another individual.

Article 7: Right to Request Access to Personal Data

Subject to the provisions of Article (16) of the Law, the Data Subject has the right to request a copy of their Personal Data in a readable and clear format, subject to the following:

1- The legal basis for processing is consent, legitimate interest of the Controller, or an agreement to which the Data Subject is a party.

2- The Personal Data is provided to the Data Subject in a commonly used electronic format. The Data Subject may request a printed hard copy if feasible.

3- When granting a Data Subject to access their Personal Data, the Controller shall ensure that it does not involve disclosing Personal Data that identifies another individual.

Article 8: Right to Request Correction of Personal Data

1- The Data Subject has the right to request correction of their Personal Data if the legal basis for processing is consent, legitimate interest of the Controller, or an agreement to which the Data Subject is a party.

2- The data subject shall have the right to obtain from the controller restriction of processing when the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data. The aforementioned restriction shall not apply if providing such data contravenes provisions of the Law and Regulations

3- The Controller may request needed supporting documents or evidence to verify in order to update, correct, or complete the Personal Data, provided that such documents or evidence are destroyed verification process is completed.

Article 9: Right to Request Destruction of Personal Data

1- Subject to the provisions of Article (18) of the Law, the Data Subject has the right to request the Destruction of their Personal Data if the legal basis for processing is consent or an agreement to which the Data Subject is a party, or the legitimate interest of the Controller.

2- The Controller shall destroy the Personal Data in any of the following cases:

a) Upon Data Subject's request, in accordance with paragraph (1) of this Article.

b) If the Personal Data is no longer necessary to achieve the purpose for which it was collected.

c) If the Data Subject withdraws their consent, and consent was the legal basis for processing.

d) If the Controller becomes aware that the Personal Data is being processed in a way that violates the Law.

3- When destroying Personal Data, the Controller shall take the following steps:

a) Take appropriate measures to notify other parties to whom the Controller disclosed the concerned Personal Data and request their Destruction.

b) Take the appropriate measures to notify the individuals to whom the Personal Data has been disclosed by any means and request its Destruction.

c) Destroy all copies of the Personal Data stored in the Controller's systems, including backups, in accordance with relevant regulatory requirements.

4- The provisions of this article shall not prejudice related legal requirements.

Article 10: Anonymization

When a Controller anonymizes the Personal Data of a Data Subject, it shall comply with the following:

1- Ensure that it is impossible to re-identify the Data Subject after Anonymization.

2- Evaluate the potential impact and risks, including the possibility of re-identifying the Data Subject, in the circumstances specified in Paragraph (1) of Article 26 of the Regulation.

3- Take the necessary organizational, administrative, and technical measures to avoid the risks identified, taking into account technological developments, methods of Anonymization, and updates to those methods.

4- Evaluate the effectiveness of the applied techniques for anonymizing Personal Data and make necessary adjustments to ensure that re-identification of the Data Subject is not possible.

Article 11: Means of Communication

The Controller is required to provide appropriate means to process requests related to Data Subject rights as stipulated in the Law. The Data Subject shall have the choice to use one or many among the following means according to their preference considering options made available by the Controller:

1- E-mail.

2- Text messages.

3- The national address.

4- Communication via electronic applications.

5- Any other communication mean provided by the Controller for this purpose.

Article 12: Consent

The Controller shall obtain the Data Subject's consent for processing their Personal Data in any appropriate form or means, including written or verbal consent or by using electronic methods, subject to the following conditions:

a) The consent shall be given freely and not obtained through misleading methods, and obtaining consent shall comply with the provisions of Article (7) of the Law.

b) The purposes of processing shall be clear and specific, and those purposes shall be explained and clarified to the Data Subject before or at the time of requesting consent.

c) The consent shall be given by a person who has full legal capacity.

d) The consent shall be documented in a way that allows verification in the future.

e) Independent consent shall be obtained for each processing operation if the purposes of processing are multiple.

The Data Subject's consent shall be explicit in the following cases:

a) When consent is the sole legal basis for processing Personal Data.

b) When the processing involves Sensitive Data.

c) When the processing involves Credit Data.

Article 13: Consent withdrawal

1- The Data Subject has the right to withdraw their consent for processing their Personal Data at any time, and they shall inform the Controller of this through any available means according to Article (5) of the Regulation.

2- Before requesting consent from the Data Subject, the Controller shall establish procedures that allow for the withdrawal of that consent and take the necessary measures to ensure their implementation, with the procedures for withdrawing consent being similar to or easier than those for obtaining it.

3- In the event of consent withdrawal, the Controller shall cease processing without undue delay from withdrawal request. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4- When the Data Subject withdraws their consent for processing their data, the Controller shall take appropriate measures to notify those to whom the Personal Data has been disclosed and request its Destruction through any available means.

Article 14: Legal Guardian

1- Considering applicable legal requirements, the legal guardian of the Data Subject that fully or partially lacks legal capacity shall act in the best interests of the Data Subject and for this purpose, they have the following options:

a) Exercise the rights granted to the Data Subject under the Law and the Regulation.

b) Consent to the processing of the Data Subject's Personal Data in accordance with the provisions of the Law and the Regulation.

2- In addition to what is stipulated in paragraph (1) of Article 12 of the Regulations, in case of processing personal data of a Data Subject that fully or partially lacks legal capacity, obtaining the consent of the legal guardian is conditional upon taking appropriate measures to verify validity of guardianship over the Data Subject.

3- Obtaining the consent from the legal guardian of a Data Subject that fully or partially lacks legal capacity shall comply with the following provisions:

a) It shall not cause any harm to the interests of the Data Subject.

b) It shall enable the Data Subject to exercise their rights as provided for in the Law and the Regulation when they reach legal capacity.

4- Considering Article (26) of the Regulation and unless the Personal Data is considered "Sensitive Data Subject to consent", the Controller may obtain the consent from a Data Subject whose ages is between 13 and 18 to processing their Personal Data without the need to obtain the consent of the legal guardian, provided that consent clause and privacy notice are written in a language and structure suitable for the targeted age group's level of understanding.

5- The consent of the legal guardian is not required in the context of services that provide direct benefit to a Data Subject that fully or partially lacks legal capacity, such as consultation or preventive services.

Article 15: Processing to Serve the Actual Interest of Data Subject

When processing data to achieve an actual interest of the Data Subject, the Controller shall retain evidence that such interest exists and that it is difficult to contact or communicate with the Data Subject.

Article 16: Collecting Data from Third Parties.

1- With the exception of what is stated in Paragraph (3) of Article (10) of the Law, when processing Personal Data collected from sources other than the Data Subject directly, the Controller shall consider the following:

   a) The processing shall be necessary and proportionate to the specified purpose.

   b) It shall not affect the rights and interests of the Data Subject.

2- When processing Personal Data in accordance with paragraph (2) of Article (10) of the Law, the Controller shall ensure that such data Collection from a publicly available source is lawful.

3- When processing Personal Data in accordance with paragraph (6) of Article (10) of the Law, the Controller shall consider the provisions of Article (10) of the Regulation regarding Anonymization.

Article 17: Processing for Legitimate Interest

1- The Controller may process personal data to achieve a legitimate interest provided that the following conditions are met:

a) The purpose shall not violate any of the laws in the Kingdom.

b) The processing shall not affect the rights and interests of the Data Subject or third parties.

c) The processing shall not conflict with the interests of Data Subjects or have negative impact on them.

d) The processing shall not include Sensitive Data.

2- Legitimate interests include the Disclosure of fraud operations, the protection of network and information security, and other legitimate interests that meet the conditions outlined in paragraph (1) of this article.

3- According to the provisions of paragraph (4) of Article (6) of the Law, before processing Personal Data for legitimate interests, the Controller shall conduct and document an assessment of the proposed processing and its impact on the rights and interests of Data Subjects. The assessment shall include the following:

a) Identification of the proposed processing and its purposes, as well as the type of data and categories of Data Subjects.

b) Evaluation of the purpose to ensure it is legitimate and compliant with the laws in the Kingdom.

c) Verification of the necessity to process Personal Data to achieve the legitimate purpose of the Controller.

d) Determination of whether the proposed processing falls within the reasonable expectations of the affected Data Subjects.

e) Evaluation of whether the proposed processing will cause any potential harm to Data Subjects.

f) Identification of any measures that shall be taken to avoid potential risks or harms, in accordance with the provisions of paragraph (2) of Article (26) of the Regulation.

4- If the assessment outlined in paragraph (3) of this article indicates that the proposed processing will in any way violate any laws, infringe on the rights and interests of Data Subjects, cause harm to them or any other party, the Controller shall modify the proposed processing and conduct a new assessment.

Article 18: Choosing the Data Processor

1- The Controller shall ensure that any data Processor chosen provides sufficient guarantees to protect Personal Data, and that the agreement with the data Processor includes the following:

a) Purpose of the processing.

b) Categories of Personal Data being processed.

c) Duration of the processing.

d) The data Processor's commitment to notify the Controller in case of a Personal Data Breach.

e) Clarification of whether the data Processor is subject to Regulations in other countries and the impact on their compliance with the laws and 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 data Processor notifies the Controller of such Disclosure.

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

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

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

4- If Processor violates the instructions issued by the Controller or the agreement regarding the processing of Personal Data, the data Processor shall be considered as a Controller and held directly accountable for any violation of provisions the Law.

5- Before entering into any subsequent contracts with data 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 afforded to the Personal Data being processed.

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

c) Obtain prior acceptance from the Controller, 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 data Processor.

Article 19: Processing of Personal Data for Secondary Use

1- When the Controller processes Personal Data for Secondary Use as provided for in Article 10 of the Law, it shall do the following:

a) Clearly and specifically define Personal Data Secondary Use purposes.

b) Document the procedures to fixe scope of data to be processed in accordance with specific purposes, including the use of data maps that indicate the need for each processed data and link it to each processing purpose.

c) Evaluate the potential negative impact and risks that may arise from the processing Personal Data, including the risks associated with the possibility of specifically identifying the identities of the Data Subjects.

d) Take necessary measures to ensure that the Personal Data is collected while respecting data minimization principle to achieve the purposes as set in paragraph (b) above.

2- With the exception of cases stated in paragraph (3) of Article 10 of the Law, when the Controller processes Personal Data for Secondary Use as provided for in paragraphs (1), (2), (4), (5), and (6) of Article 10 of the Law, the Controller shall comply with the following:

a) Clearly and accurately define the purpose of the processing and refer to it in the records of Personal Data processing activities.

b) Limit the Collection and processing of the Personal Data to the minimum amount necessary to achieve the purpose.

c) Identify the type of Personal Data to be processed and the necessary measures to ensure that such data is processed appropriately.

Article 20: Data Minimisation

1- The Controller shall collect only the minimum amount of Personal Data necessary to achieve the purpose of the processing, and ensure the following:

a) Collecting only the necessary Personal Data that is directly related to the purpose of processing, which is determined by using data maps that indicate the need for each collected data and link it to each objective of the processing or other means.

b) Provide necessary care to achieve the purpose of the processing without collecting unnecessary Personal Data.

c) Document the procedures for identifying the Personal Data to be processed for any specific purpose by the Controller, in accordance with the controls set out in this article.

2- The Controller shall retain the minimal Personal Data necessary to achieve the purpose of the processing.

Article 21: Disclosure of Personal Data

1- Disclosure of data collected from publicly available sources under paragraph (2) of Article 15 of the Law requires that the Collection of such data from a public source to be Lawful.

2- Except for the circumstances provided for in paragraphs (3) and (4) of Article 15 of the Law, the Controller 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.

3- When disclosing Personal Data in response to a request from a public authority for security purposes, or to implement another system, or to satisfy legal requirements, the Controller shall do the following:

a) Document the request for Disclosure.

b) Accurately identify the type of Personal Data required to be disclosed.

4- Except as provided in paragraphs (3) and (4) of Article 15 of the Law, when disclosing Personal Data related to another person who is not the data subject, the controller shall take necessary care and provide sufficient guarantees to ensure the privacy of the other individual is preserved and not violated. This includes taking the following steps:

a) Pseudonymisation of Personal Data that directly or indirectly identifies the other person or anonymising the identity of the Data Subject.

b) Obtain the consent of the other person to disclose the data after evaluating the negative impact and potential risks that may arise from the other person being aware of the Disclosure request, and who was not aware of the link between their data and the Personal Data of the Data Subject or it was not appropriate for them to know.

c) Balance between the rights of the data subject and the rights of any other person in each case separately.

5- When disclosing Personal Data to achieve a legitimate interest of the Controller, the Controller shall comply with the provisions of Article 17 of the Regulation.

6- The Controller shall include Disclosure operations in the records of data processing activities, document the dates, methods, and purposes of Disclosure.

Article 22: Controls for Processing Personal Data for Public Interest Purposes

When a Public Entity collects Personal Data not directly from the Data Subject, processes it for Secondary Use, or requests Disclosure of such data to achieve a public interest, the Public Entity shall comply with the following:

1- Ensure that it is necessary to achieve a clearly defined public interest.

2- That the public interest is related to the mandate as specified by law.

3- Take suitable measures to limit the damage that may result.

4- Record those operations in the records of Personal Data processing activities.

Article 23: Correction of Personal Data

1- The types of correction of Personal Data referred to in paragraph (2) of Article 17 of the Law include correcting data that is incorrect, completing data that is incomplete, or updating data that is outdated.

2- When correcting Personal Data, the Controller shall comply with the following:

a) Ensure the accuracy and integrity of Personal Data by examining and reviewing supporting documents if necessary.

b) Notify the parties to whom the Personal Data has been disclosed previously without delay.

c) Notify the Personal Data Subject when the correction is completed.

d) Document all updates made to Personal Data.

3- If the Controller identifies that Personal Data is inaccurate or incomplete, and that may cause harm to the Data Subject, the Controller shall suspend processing until the data is updated or corrected.

4- In accordance with paragraph (2) of this Article, when the Controller becomes aware that Personal Data is inaccurate, outdated, or incomplete, the Controller shall take the necessary steps to correct, complete, or update it using the available means within no more than (thirty) days from the date of becoming aware of the issue.

5- The Controller shall take appropriate measures to avoid the impact of processing inaccurate, incomplete, or outdated Personal Data, including:

a) Develop and update internal policies and procedures in accordance with the provisions of the Law and Regulations, including procedures that enable Data Subjects to exercise their right to request correction in accordance with the provisions of the Law and Regulations.

b) Periodic review of the accuracy and timeliness of Personal Data.

Article 24: Information Security

The Controller shall take the necessary organizational, administrative, and technical measures to ensure the privacy of the Data Subject and the security of Personal Data, and shall comply with the following:

a) Implement appropriate security and technical measures to limit security risks related to Personal Data.

b) Comply with relevant controls, standards, and rules issued by the National Cybersecurity Authority or recognized best practices and cybersecurity standards if the Controller is of a special nature.

Article 25: Notification of Personal Data Breach

1- The Controller shall notify the Competent Authority within a delay not exceeding (72) hours of becoming aware of the incident, if such incident potentially causes harm to the Personal Data, or to Data Subject or conflict with their rights or interests. the notification shall include the following:

a) A description of the Personal Data Breach incident, including the time, date, and circumstances of the breach and the time when the Controller became aware of it.

b) Data categories, actual or approximate numbers of impacted Data Subjects, and the type of Personal Data.

c) A description of the risks of the Personal Data Breach, including the actual or potential impact on Personal Data and Data Subjects, and the actions and measures taken by the Controller to prevent or limit the impact of those risks and mitigate them, as well as the future measures that will be taken to avoid a recurrence of the breach.

d) A statement if the Data Subject has been notified of the breach of their Personal Data, as stipulated in Paragraph (5) of this Article.

e) The contact details of the Controller or its data protection officer, if any, or any other official who has information regarding the reported incident.

2- If the Controller is not able to provide any of the required information within (72) hours from the time it became aware of the Personal Data Breach in accordance with paragraph (1) of this article, it shall provide it as soon as possible, along with justifications for the delay.

3- The Controller shall keep a copy of the reports submitted to the Competent Authority under paragraph (1) of this article and document the corrective measures taken in

relation with the Personal Data Breach, as well as any relevant documents or supporting evidence.

4- The provisions of this article do not prejudice the obligations of the Controller or Processor to submit any report or notification about Personal Data Breaches according to what is issued by the National Cybersecurity Authority or any laws and Regulations applicable in the Kingdom.

5- The Controller shall, without undue delay, 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, and that it includes the following:

a) A description of the Personal Data Breach.

b) A description of the potential risks arising from the 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 Controller and its data protection officer, if any, or any other appropriate means of communication with the Controller.

d) Any recommendations or advice that may assist the Data Subject in taking appropriate measures to avoid the identified risks or limit their impact.

Article 26: Assessment of Potential Impacts and Risks

1- The Controller shall prepare a written and documented assessment of the potential impacts and risks that may affect the Data Subject as a result of the processing. Risk assessment shall be conducted in the following cases:

a) Processing of sensitive Personal Data.

b) Collecting, comparing, or linking two or more sets of Personal Data obtained from different sources.

c) The activity of the Controller includes – systematic 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.

d) Providing a product or service that involves processing Personal Data that is likely to cause serious harm to the rights, and privacy of Data Subjects.

2- The risk assessment shall include at least the following elements:

a) The purpose of the processing and its legal basis.

b) A description of the nature of the processing to be conducted, the types and sources of Personal Data to be processed, and any entities to whom the Personal Data is to be Disclosed.

c) A description of the scope of the processing, which identifies the type of Personal Data and the geographical scope of the processing.

d) A description of the context of the processing, which identifies the relationship between the Data Subjects, the Controller, and the Processors, as well as any other relevant circumstances.

e) An assessment of the necessity and proportionality of the processing, which identifies the measures to be taken to enable the Controller and Processors to

process the minimal Personal Data necessary to achieve the purposes of the processing.

f) The impact of the processing, based on the 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 the likelihood of their occurrence.

g) The measures that will be taken to prevent or limit the magnitude of identified risks.

h) An evaluation of the suitability of the measures envisaged to avoid identified risks.

3- The Controller shall provide a copy of the risk assessment to any Processor acting on its behalf in relation to the relevant processing.

Article 27: Processing of Health Data

The Controller shall take the appropriate organizational, technical, and administrative measures to safeguard Health Data from any unauthorized use, misuse, use for purposes other than for which it was collected, or breach, and any procedures or means that

guarantee the preservation of the privacy of its owners, and it shall, in particular, take the following controls and procedures:

1- Adopt and implement the requirements and controls issued by the Ministry of Health, the Saudi Health Council, the Saudi Central Bank, the Council of Health Insurance, and other related entities involved in regulating Health Services and health insurance services, that specify the tasks and responsibilities of employees of health care providers, health insurance companies, health insurance claims management companies and those which are contracted by them carrying out the processing of Health Data.

2- Include the provisions of the Law and Regulation in the code of conduct for the Controller's employees.

3- Distribute tasks and responsibilities among employees or workers in a way that prevents overlapping specializations and diffusion of responsibility, and taking

into account different level of access to data among employees or workers in a manner that guarantees the highest degree of privacy protection.

4- Document all stages of Health Data processing and provide the means to identify the person in charge for each stage.

5- The agreement between the Controller and the Processors -to conduct work or tasks related to the processing of Health Data- shall include provisions that oblige them to abide by the procedures and measures stated in this Article.

6- Health Data processing of should be limited to the minimum data necessary to provide healthcare services and products or health insurance programs.

Article 28: Processing of Credit Data

Without prejudice to the provisions of the Credit Information Law and its implementing Regulations, the Controller shall take organizational, technical, and administrative measures to safeguard Credit Data from any unauthorized use, misuse, access by

unauthorized individuals, use for purposes other than for which it was collected, and Disclosure. The Controller shall adopt the following controls and procedures:

1- Adopt and implement requirements and controls issued by the Saudi Central Bank and other relevant authorities, which define the roles and responsibilities of

employees of establishments providing credit information services and of the parties that have contracts with such establishments to processing Credit Data.

2- For Processors conducting activities involving credit data processing, include in the agreement a clause request obliging them to follow the provisions of this article.

3- The Controller shall obtain the consent of the Data Subject and notify them of any request to disclose their Credit Data in accordance with the provisions of the Credit Information Law.

Article 29: Processing of Data for Advertising or Awareness Purposes

1- The Controller shall obtain Explicit Consent from the targeted recipient before sending advertising or awareness material in case there is no prior interaction between the Controller and the targeted recipient.

2- The conditions for obtaining the targeted recipient's consent for advertising or awareness materials shall be as follows:

a) The consent shall be given freely, and no misleading methods shall be used to obtain it.

b) The targeted recipient shall be enabled to specify the options related to advertising or awareness material subject to consent.

c) Consent of a targeted recipient consent shall be documented in a manner that can be verified in the future.

3- Before using communication methods for the purpose of sending advertising or awareness materials, including post and email of the Data Subject, the Controller shall commit to the following:

a) Clarify the method used to send advertising or awareness materials to the targeted recipient.

b) Clearly mention sender's name without hiding their identity in all advertising or awareness messages.

c) Provide to targeted recipient a mechanism to stop receiving such materials that is quick and easy to activate whenever desired. The procedures to stop receiving the advertising or awareness materials shall be as easy as the procedures to obtain consent.

d) Stop sending advertising or awareness messages as soon as the targets recipient requests it.

e) The cessation of receiving advertising or awareness materials shall be free of charge.

f) Keep material evidence of consent from the targeted recipient to receive advertising or awareness material.

Article 30: Direct Marketing

1- Before processing Personal Data for Direct Marketing purposes, the Controller shall abide by to the following:

a) Obtain consent from Data Subject in accordance with the provisions of Article (12) of the Regulation.

b) Inform the Data Subject, when obtaining their consent, of the types of Personal Data that will be used for Direct Marketing.

c) Provide a mechanism that allows the Data Subject to withdraw their consent for the processing of their Personal Data for Direct Marketing purposes, and to stop

receiving related marketing materials at any time, provided that the mechanism is simple, fast, free of charge, and the procedures for withdrawing consent are similar or easier than the procedures for obtaining it.

d) Comply with the requirements issued by the relevant authorities on marketing and obtain the necessary licenses in cases that require it.

2- When sending Direct Marketing messages to a Data Subject, the identity of the Controller shall be clearly stated without any misleading information.

3- The Controller shall keep records that include consent of Data Subjects to receive Direct Marketing, indicating the time and method of consent.

4- In case the Data Subject withdraws their consent for Direct Marketing, the Controller shall immediately stop sending related marketing materials without undue delay.

5- The transmission of Direct Marketing material shall be from the entity to which consent was given by the Data Subject, and not by a third party, unless the consent

was obtained by that third party after informing the Data Subject of the sender and the purpose of the marketing.

Article 31: Collection and Processing of Data for Scientific, Research, or Statistical Purposes

When collecting and processing Personal Data for scientific, research, or statistical purposes without the consent of the Data Subject, the Controller shall commit to the following:

a) Clearly and accurately specify the scientific, research, or statistical purposes.

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

c) Take the necessary measures to ensure that the processing does not have any negative impact on the rights and interests of the Data Subject.

Article 32: Photographing or Copying Official Documents that Reveal the Identity of Data Subjects

Without prejudice to the relevant laws, the Controller shall refrain from photographing or copying official documents -issued by Public Entities- where Data Subjects are identifiable, except upon request from a public Competent Authority or when required by Law. The Controller shall provide the necessary protection for such documents and

destroy them once the purpose for which they were obtained has ended unless there is a legal requirement to keep them.

Article 33: Transfer or Disclosure of Data to Entity outside the Kingdom

The Transfer or Disclosure of Personal Data to entity outside the Kingdom shall be carried out in accordance with the provisions of the Law and the Regulation of Personal Data Transfer outside the geographic borders of the Kingdom.

Article 34: Data Protection Officer

1- The Controller shall appoint one or more individuals to be responsible for the protection of Personal Data in any of the following cases:

a) The Controller is a Public Entity that provides services that involve processing of Personal Data on a large scale.

b) The primary activities of the Controller consist of processing operations that require regular and systematic monitoring of individuals on a large scale.

c) The core activities of the Controller consist of processing sensitive Personal Data.

2- Subject to the requirements of paragraph (1) of this Article, the data protection officer may be an official, an employee or an external contractor of the Controller.

3- The Competent Authority shall issue rules for the appointment of the data protection officer, which shall include the circumstances under which a data protection officer shall be appointed, as well as their duties and responsibilities.

Article 35: Records of Personal Data Processing Activities

1- The Controller shall keep a record of Personal Data processing activities during the period of its activity related to Personal Data processing, in addition to the following periods:

a) Three years starting from the date of termination of the Controller's activity, for controllers whose activities involve processing Personal Data on a large scale or on a regular basis for individuals that fully or partially lack legal capacity, or for processing activities that require continuous monitoring of Data Subjects, or for processing Personal Data using new technologies, or for making decisions based on automated processing of Personal Data.

b) One year for controllers not concerned by cases stated in subparagraph (A) of paragraph (1) of this Article.

2- Records of Personal Data processing activities shall be written.

3- The Controller shall ensure that the records of Personal Data processing activities are accurate and up to date.

4- The Controller shall provide access to the records of Personal Data processing activities to the Competent Authority upon request.

5- The Competent Authority shall provide templates of records of Personal Data processing activities.

Article 36: National Register of Controllers

The Competent Authority shall issue the rules for registration in the National Register of Controllers, provided that the rules include the controllers that are required to register.

Article 37: Accreditation bodies

The Competent Authority shall issue the regulatory rules for licensing entities that issue accreditation certificates for controllers and Processors in accordance with paragraph (2) of Article 33 of the Law.

Article 38: Licensing of Audit Entities

1- The purpose of audit and checking is to ensure that the entity is properly protecting Personal Data through auditing and checking of carried out Personal Data processing activities, and related controls and procedures, and identifying any gaps in compliance with the Law and Regulations.

2- Entities licensed to carry out audit or examination of Personal Data processing activities shall perform according to the following:

a) Provide services and products independently according to professional standards.

b) Develop the necessary administrative and organizational procedures and controls to ensure the accuracy and integrity of their output.

3- The Competent Authority shall issue the rules for licensing entities that undertake auditing or examination of Personal Data processing activities in accordance with paragraph (3) of Article 33 of the Law.

Article 39: Filing and Processing Complaints

1- The Data Subject may complain to the Competent Authority within a period not exceeding (90) days from the date of the incident or the date on which the Data Subject became aware of it. The Competent Authority shall determine whether to accept the complaint or not after this period in cases where there are reasonable

causes that may have prevented the Data Subject from submitting the complaint in time.

2- The Competent Authority shall receive the complaints that are submitted to it, according to procedures that ensure celerity and quality.

3- The Competent Authority shall keep a record of the complaints filed against those suspected of violating provisions of the Law, taking into account the guarantees that ensure the privacy of complainants.

4- The complaint shall include the following information:

a) The place and time of the violation.

b) The name, identification, address, and telephone number of the complainant.

c) Information about the complained entity.

d) A clear and specific description of the violation, along with the evidence and the information provided with the complaint.

e) Any other requirements specified by the Competent Authority.

5- The Competent Authority shall examine and study the complaints, their documents and the evidence provided, and may communicate with the complainant for clarification as needed to request the relevant documents and information.

6- The Competent Authority shall take the necessary measures regarding the complaints submitted to it and inform the complainant of the outcome.

7- The Competent Authority shall issue procedural evidence for processing complaints.

8- The Competent Authority shall maintain an internal record of the complaints filed with it in accordance with the provisions of Article 34 of the Law and this Article.

Article 40: Publication and Enforcement

The Regulation shall be published in the official gazette and on the official website of the Competent Authority and shall come into force from the date of the Law's enforcement.