Draft of the Executive Regulation of Personal Data Protection Law (PDPL)

Chapter I: Definitions

Article 1 - Definitions

The terms and phrases used in the Regulations shall have the meanings set out in Article 1 of the Personal Data Protection Law issued by Royal Decree No. M/19, dated 9/2/1443 AH, in addition to the following meanings, unless the context requires otherwise:

Law: Personal Data Protection Law.

Regulation: The Executive Regulations of the Law.

Regulatory Authority: Any government authority or any entity that has independent public personality and has, in accordance with its powers and responsibilities, regulatory or oversight duties and responsibilities over a certain sector or activity in the Kingdom.

Direct Marketing: Communication, via any means, with a person or a group of persons, aiming to send marketing, advertising or awareness-raising material to such person or group.

Practical Need: Actual need for processing of personal data, with fairness and integrity and without conflicting with the rights and expectations of the Personal Data Subject.

Personal Data Breach: Any act in any manner that leads to illegal disclosure of Personal Data, whether it is intentional or not.

Risks and Impact: The possibility that Personal Data Subject may suffer damage due to processing of their Personal Data, and the impact of such risk.

Anonymization: Removing any direct or indirect characteristics from the Personal Data, that may make the Personal Data Subject specifically identified.

Transfer of Personal Data to outside the Kingdom: Sending or sharing Personal Data, via any means, to or with an entity outside the Kingdom, in order to process such Personal Data fully or partially, for specific purposes based on legal justification or Practical Need.

Codes of Conduct: A set of general rules and specific responsibilities approved by the Regulatory Authority, which Controllers and Processors are obligated to comply with, to face the challenges relating to protection of Personal Data in a specific sector, in order to establish a system of proper practices in that sector and to comply with that system.

Profiling: Automated Processing of Personal Data and using such Personal Data to analyse and assess certain personal aspects of the Data Subject, and to forecast aspects relating to the Data Subject's performance at work, financial status, health, personal preferences, interests, behaviour, location or movement, for the purpose of creating a profile of the Data Subject.

Special Categories: Individuals or groups that need special care, support or protection due to age or sickness, or those who are vulnerable to abuse or negligence.

Explicit Consent: Verbal or written consent that is express, specific and given freely by the Data Subject, proofing that the Data Subject agrees to process their Personal Data.

Implied Consent: Consent that is not given Explicitly by the Data Subject or the authorized person, but given implicitly through the person's actions and the facts and circumstances of the situation.

Article 2 – Location Data

The location data mentioned in paragraph 11 of Article 1 of the Law means data that is collected and processed through a public telecommunications network or service and indicate the geographical location of the devices of users or subscribers, including geographical location coordinates, user's movement routes or directions, and the date and time of recording the location data.

Article 3 - Scope of Application

The personal and family use referred to in Article 2 of the Law means the processing personal data by an individual within their family or within their limited social circle taking part in any social or family activity. This shall not apply where an individual publishes Personal Data to the public or discloses Personal Data to any person outside their family or outside the aforementioned social circle, or where an individual uses Personal Data for any professional, non-profit or commercial activity.

Chapter II: Rights of Personal Data Subject

Article 4 - Right to Know

Before or during collecting Personal Data, the Controller shall:

1. Inform the Personal Data Subject of the following:
    a. Controller's name, contact details, and relevant available channels.
    b. Content of the Personal Data that need to be processed, purpose of processing, legal justification or Practical Need, and the periods for which the data will be kept.
    c. Data collection methods, data processing means and how the data will be used.
    d. The entities with which the data will be shared.
2. Inform the Personal Data Subject of the data sources if the Personal Data are to be collected —in a lawful manner— from a source that is not publicly available.
3. Set a privacy policy, review that policy regularly, update the policy whenever the need arises, notify the Personal Data Subject of any update to the policy and obtain the Personal Data Subject's consent before starting any processing for new purposes.

Article 5 - Right to Know on Using Emerging Technology

Without prejudice to Article 13 of the Law, when using modern or emerging technology, such as artificial intelligence, the Controller shall inform the Personal Data Subject of the following:

1. The content of the Personal Data to be collected and processed, including the data that is processed subsequently by the Controller.
2. The methods and means of collecting and processing Personal Data, and how those methods and means are used.
3. The periods for which Personal Data will be kept.
4. Sufficient information on the automated decision-making mechanism, if any, in plain and clear language.
5. The methods and means available to request human intervention, object to automated decisions, or express the Data Subject's point of view.
6. The contact details of the Personal Data protection officer, if there is one.

Article 6 - Right to Request Access or Copy

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

1. Verify the identity of the Personal Data Subject or their representative before enabling them to access their data or obtain a copy thereof.
2. The foregoing shall be conducted in a secure, easy and clear manner, and shall include all the data which the Controller keeps concerning the Personal Data Subject as has been collected directly from the Personal Data Subject.
3. Not disclose any Personal Data that identifies any other person. Where that is not possible, the consent of the other person shall be obtained. Article 26 of this Regulation shall be observed.
4. If the request is made repeatedly and requires unreasonably extraordinary efforts by the Controller, the Controller may request a reasonable fee for providing the Personal Data Subject with a copy of their personal data.

Article 7 - Right to Request Correction

Subject to Article 17 of the Law, when correcting or completing Personal Data, or updating Personal Data at the request of the Personal Data subject, the Controller shall:

1. Verify the identity of the Personal Data Subject or their representative.
2. 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.
3. 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.

4. Notify the Personal Data Subject upon the correction, completion or updating of their data, and lift the restrictions imposed on processing.
5. 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.
6. Document all the updates made to the Personal Data.

Article 8 - Right to Request Destruction

1. Subject to Article 18 of the Law, the Controller shall destroy Personal Data at the written request of the Personal Data Subject in the following cases:
   a. If the data becomes no longer necessary for the purpose for which it has been collected.
   b. If the personal data subject withdraws their previous consent to the collection of their data and that consent was the legal basis for the processing.
   c. If the Practical Need is the grounds on which the Personal Data processing is based and the Personal Data Subject objects to the processing and there is no interest outweighing the rights of the Personal Data Subject requiring the continuation of the processing.
   d. If Direct Marketing is the purpose for which the data under the destruction request is processed.
   e. If the data under the destruction request has been processed in a manner not consistent with the Law.
2. When destroying Personal Data, the Controller 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 Controller, whether archived data or backup copies, in accordance with the timeline and procedures set by the Controller.

Article 9 - Communication, Duration and Documentation Provisions Relating to Requests of Personal Data Subjects

1. Controller shall 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 needs of Special Categories.

2. Controller shall carry out the request of Personal Data Subject within 30 days of receiving the request. If carrying out the request requires unreasonably extraordinary efforts or the Controller receives multiple requests from the same Personal Data Subject, the Controller may extend the period by not more than 30 additional days, provided the Controller shall notify the Personal Data Subject of such extension and the justifications therefor.
3. Controller shall document and keep the details of the requests it receives, including any verbal requests.

Article 10 – Means of Communications and Notifications

1. Notification and communication between the Controller and Personal Data Subject shall take place through one or more of the following means as the Personal Data Subject may decide:
    a. Text messages sent to authenticated mobile phones.
    b. Accounts registered in government automated systems.
    c. The post.
    d. Applications' notifications and alerts.
    e. Any other electronic means designated for that purpose and recognized in the Kingdom.
2. Notification and communication through the method(s) chosen from the foregoing shall be valid and effective, unless the Personal Data Subject make a notification of changing such method(s) in the form designated for that purpose.

Chapter III: Provisions Concerning Consent and Personal Data Collection and Processing

Article 11 - Consent

The interest mentioned in the first paragraph of Article 6 of the Law means any interest of material importance to the physical, psychological, moral or financial safety of the Personal Data Subject.

Except in the cases referred to in Article 6 of the Law; before or during collecting Personal Data directly from the Personal Data Subject for processing (or for changing the purpose of Processing), the Controller shall obtain consent by any appropriate means or in any appropriate form, including by means of written consent forms, electronic forms, settings in applications, verbal consent or Implied Consent if allowed, provided the following shall be taken into account:

1. Obtain and document Explicit Consent in a manner that can be proven in the future; after notifying the Personal Data Subject of the consent purpose and legal justification or Practical Need, informing the Personal Data Subject of the options available, and informing the Personal Data Subject that the processing will be limited to the minimum amount of Personal Data necessary to achieve the purpose, and that the Personal Data

Subject has the right to withdraw their consent at any time, provided the Controller shall observe the following:

a. If the processing has multiple purposes, the consent to processing the relevant data shall be taken after clearly differentiating between all of the processing operations.

b. In the event of Sensitive Data, the consent shall be in writing.

c. The consent shall be in writing and made by the legal guardian or legal representative in the event of processing data belonging to a person that is fully or partially incompetent or is deceased, unless the purpose of the processing is related to a preventive or advisory service for the safety of that person.

2. Establish and implement procedures for the Personal Data Subject to withdraw consent, provided such procedures shall be similar to or easier than the procedures for obtaining the consent.

3. The consent may be implied if the Personal Data Subject is clearly informed of the processing and it is not reasonably possible to request Explicit Consent from the Personal Data Subject, and the action of the Personal Data Subject clearly and unambiguously affirms that the Personal Data Subject consents to the processing.

Conditions for obtaining consent to processing Personal Data of children:

a. Consent of any person under the age of 13 may only be given by the legal guardian of such person.

b. Controller may obtain the consent of persons aged between 13 and 18 in accordance with the following conditions:

(a) The request for the consent and for any other information relating to the consent shall be in made in language suitable for the age of the person.

(b) It is appropriate to expect the person in the age group, to whom the processing activities of the Controller relate, to be aware of the consequences of the processing.

1. In the event the Controller obtains consent related to a child, the Controller shall be responsible for proving the following upon the request of the Competent Authority:

a. It was appropriate to expect the person in the age group, to whom the processing activities of the Controller relate, to be aware of the consequences of the processing.

b. The consent is consistent in all aspects with the requirements of the Law and regulations.

Article 12 - Advertising and Awareness-Raising Provisions Concerning Marketing

1. Before using personal means of communication, including postal and electronic addresses, of Personal Data Subject to send advertising or awareness-raising material, the Controller shall observe the following:

    a. Obtain Explicit Consent of the target Personal Data Subject. Implied Consent shall not be valid, as consent shall be given by an act that can be documented.

    b. Inform the Data Subject of the means of sending the advertising or awareness-raising material.

    c. Provide and make clear a mechanism for the Data Subject to stop receiving such material quickly and easily whenever the Data Subject decides.

    d. Stop sending the advertising or awareness-raising material shall be free of charge.

    e. Adhere to the related authorities' requirements and rules concerning advertising, and obtain the necessary licenses.

    f. Clearly state the sender's name, without concealing the sender's identity in any manner, in every advertising or awareness-raising message.

    g. Keep records of the times and methods of consent of Data Subjects.

    h. Sending shall be by the entity to which the Data Subject has given the consent, not by any third party, unless the consent was obtained by that third party after it has made clear to the Personal Data Subject the identity of the sender and the purpose of sending, and after the entity has verified that the Explicit Consent of the Data Subject had been obtained in accordance with provisions of this Article.

2. Neither the provisions contained in privacy policies on obtaining the consent of Data Subject to receiving advertising or awareness-raising messages, nor requests for consent that are written in an unclear manner, shall be valid.

3. Controller shall stop sending advertising or awareness-raising messages as soon as it receives request from the Data Subject to stop sending such messages.

Article 13 - Collection and Disclosure of Data for Security Purposes, in Implementation of Another Law, or to Fulfill Judicial Requirements

1. The following conditions shall apply where a public Controller collects Personal Data from a person other than the Data Subject, or processes Personal Data for a purpose other than the purpose for which the Personal Data has been collected for security reasons, to implement another law or to fulfill judicial requirements:

    a. The purpose of the processing shall be clearly and precisely defined, and shall be directly related to the purpose for which the Personal Data has been collected.

    b. The content of the required Personal Data shall be limited to the minimum necessary to achieve the purpose.

c. The type of the Personal Data sought to be processed, and the measures necessary to ensure that such Personal Data is used in the required manner, shall be identified.

2. The following conditions shall apply where a Controller discloses Personal Data at the request of a Public Entity for security purposes, to implement another law or to fulfill judicial requirements:

   a. The Controller shall document the disclosure request.

   b. The type of the Personal Data sought to be disclosed, and the measures necessary to ensure that such Personal Data is used in the required manner, shall be identified.

Article 14 - Processing Personal Data of Anonymized Data Subject

When processing Personal Data in a way through which the Personal Data Subject cannot be identified directly or indirectly, the Controller shall observe the following controls and procedures:

1. Adopt means and methodologies to assess the potential risks and adverse impact that may result from the processing of such Personal Data, including the possibility of identifying the Data Subject specifically.
2. Apply the necessary organizational, administrative and technological means and measures to avoid the potential risks or to limit their impact if they occur.
3. Take into account the factors related to the context of the processing when assessing potential risks, and the factors surrounding the processing both internally and externally, including social and technological factors.
4. Take into account the rapid development in technology and the ability to use appropriate means and techniques to anonymize identity.
5. Assess the efficiency and effectiveness of the means used to anonymize the identity of the Personal Data Subject, in order to ensure that the identity cannot be specifically identified.

Article 15 - Collecting and Processing Data Using Automated Decision-Making Means

If achieving the purpose of collecting Personal Data requires that the Personal Data be processed in an automated manner that results in automated decision-making without human interference, including Profiling for marketing purposes, the Controller shall:

1. Conduct an impact assessment to identify and evaluate potential risks and adverse effects before starting the making of automated decisions concerning Personal Data Subjects, and to determine how to avoid or limit such potential risks and adverse effects.
2. Notify the Data Subject of the necessary information concerning the mechanism of processing Personal Data and automated decision-making.
3. Provide appropriate means to enable the Personal Data Subject to request human intervention to review the decisions automatically made.

4. Provide appropriate means to enable the Personal Data Subject to express their point of view concerning the mechanism of decision-making or concerning objecting to such mechanism, or to make a complaint.
5. Apply means and procedures as necessary and appropriate to ensure that the decision-making automated systems operate in the desired manner, without any bias or discrimination, and review and audit that process periodically.
6. Anonymize the identity of the Personal Data Subject when used in a Profiling activity.

Article 16 - Data Collection for Scientific, Research or Statistical Purposes without Consent of Data Subject

Subject to Article 11 of the Law, when collecting or processing Personal Data for scientific, research or statistical purposes without consent of the Data Subject, the Controller shall observe the following:

1. Identify the scientific, research or statistical purposes clearly and accurately.
2. 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.
3. The data to be collected or processed shall not include anything that specifically indicates the identity of the Data Subjects.
4. 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.

Article 17 – The Minimum Related to Personal Data Collection and Processing

The minimum of the Personal Data content shall be determined according to the following:

1. The content shall be appropriate and necessary for achieving the specified purpose and directly related to that purpose.
2. The amount of Personal Data shall be limited to what is actually necessary to achieve the purpose, without collecting any additional data.
3. Due care shall be exercised to reasonably benefit from the technological capabilities that help achieve the purpose without collecting unnecessary data.
4. The procedures for determining the content of the Personal Data shall be documented in accordance with the specific purposes and the controls referred to in this Article.

Chapter IV: Provisions Relating to Contracting between Controller and Processor, and Subsequent Contracts

Article 18 - Contract between Controller and Processor, and Subsequent Contracts

When contracting with a Processor, the Controller shall:

1. Choose the entity that is the most efficient in providing the guarantees necessary to protect Personal Data, and provide all measures necessary to protect Personal Data from any illegal processing, including to conduct risk assessment on the processing of Personal Data, as determined by the Competent Authority.
2. Obtain the required approvals from Regulatory Authorities.
3. Include the following in the contract with the Processor:
    a. The subject-matter and purpose of the processing, and the category and type of the Personal Data to be processed.
    b. The term of the contract, and the rights and obligations of each party, which shall include to:
        (1) Immediately inform the Controller of any actual or potential Data Breach, or damage or unauthorized access to Personal Data.
        (2) Obtain the approval of the Controller if the Processor wishes to enter into a contract with another party for processing of Personal Data.
        (3) Abide by any conditions set by the Competent Authority.
4. Verify that the Processor complies with the Law, regulations and instructions, and visit the Processor's premises to conduct audits and review records and periodic reports in proportion to the risks associated with the processing. The controller may delegate other parties in this regard, provided such delegation shall not exempt the Controller from its responsibilities in that respect.
5. The processing instructions issued by the Controller to the Processor shall be written and documented. That includes the communications between the two parties.
6. The provisions of this Article shall apply to all subsequent contracts of the Processor.

Chapter V: Provisions Relating to Safeguarding, Disclosure and Breach of Personal Data

Article 19 - Information Security

The Controller shall apply such organizational, administrative and technological means and measures so as to ensure privacy of Personal Data Subjects at all the stages where their Personal Data is dealt with, used and transferred. That shall include the following:

a. Assess the potential risks and adverse effects, in accordance with Article 27 of this Regulation, 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 Controller is located outside the Kingdom, the Controller shall adopt the international best practices and the best standards widely in use in relation to cybersecurity.

Article 20 - Controls and Procedures for Dealing with Health Data

The Controller 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. The Controller shall in particular apply the following controls and measures:

1. Adopt and implement the 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, which identify the tasks and responsibilities of the employees of health care providers, health insurance companies and health insurance claim management companies and the parties with which they enter into contracts if such parties engage in processing of Health Data.
2. Prevent access by any entity or individual to such data, other than the medical team assigned to the case and the employee tasked with entering and processing such data, and only to the extent needed.
3. 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.
4. Incorporate into the Controller's employee codes of conduct the general rules contained in the Law and regulations.
5. Assign tasks and responsibilities among employees in such a manner so as to prevent overlap of roles or indefinite distribution of the responsibility for protection of Health Data, and ensure gradual access to data among employees, in order to ensure the highest level of data protection.
6. Document all the stages of processing of Health Data, provide means to identify the employee responsible for each stage of processing, and limit access to the minimum number of employees required.
7. State in the contracts entered into between the Controller and 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.

Article 21 - Controls and Procedures for Dealing with Credit Data

Without prejudice to the Credit Information Law and its Executive Regulation, the Controller shall apply such organizational, technological, technical and administrative means and measures as sufficient to protect Credit Data from any unauthorized use, misuse, unauthorized access, use for any purpose other than that for which such data has been collected, breach or destruction. The Controller shall apply, in particular, the following controls and measures:

1. Adopt and implement the requirements and controls issued by the Saudi Central Bank, the Capital Market Authority, the Zakat, Tax and Customs Authority and related authorities, which identify the tasks and responsibilities of the employees of the establishments that provide financial products and services and the parties they contract with if such parties are engaged in processing of Credit Data.
2. Notify the Credit Data Subject when a request for disclosing their data is received from any entity, and not collect such data or change the purpose of collecting or publishing such data without the prior written consent of the Data Subject, in accordance with the provisions of the Law, regulations and Credit Information Law.
3. Ensure that the employees engaged in processing of Credit Data are honest and responsible and have them sign a non-disclosure agreement in relation to the said data.
4. Incorporate into the Controller's employee codes of conduct the general rules contained in the Law and regulations.
5. Assign tasks and responsibilities among employees in such a manner so as to prevent overlap of roles or indefinite distribution of the responsibility for protection of Credit Data, and ensure gradual access to data among employees, in order to ensure the highest level of data protection.
6. Document all the stages of processing Credit Data, provide means to identify the employee responsible for each stage of processing, and limit access to the minimum number of employees required.
7. State in the contracts between the Controller and Processors for carrying out of work or tasks related to processing of Credit Data, provisions that obligate them to follow the foregoing means and measures.

Article 22 - Copying and Photocopying Official Documents Identifying their Subject

The Controller may not copy or photocopy official documents —issued by Public Entities— that identify the Personal Data Subject except, if the Controller is a Public Entity, based on a requirement that is among the Controller's duties under its regulations, unless to carry out a legal requirement, or unless based on instructions given to the Controller by a Public Entity that has the authority to do so. In all cases, the Controller shall notify the Data Subject before copying or photocopying their official documents, stating the legal justification, provide the necessary protection for such official documents, and, unless there is a legal requirement to keep such documents, destroy the documents immediately once the purpose in question ends.

Article 23 - Notifying the Competent Authority of Data Breach

1. The Controller shall promptly, and in any event no later than 72 hours, notify the Competent Authority of any Breach or damage or unauthorized access to Personal Data. Such notification shall be accompanied by a report that includes the following:
    a. An analysis of the 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 Controller, and the contact details of the Personal Data protection officer, if any, or of any other official that has information concerning the incident.

2. If the Controller is unable to provide complete information within 72 hours since becoming aware of the incident, or if there is not enough information available, such information may be provided subsequently as it becomes available, along with the related justification.

3. The Controller shall keep and document the incident facts and effects, and the procedures taken in relation to the incident.

4. The provisions of this Article shall be without prejudice the Controller's obligations of reporting or notification under any applicable laws.

Article 24 - Notifying Personal Data Subject of Data Breach

1. In the event of actual or potential Data Breach, or actual or potential damage or unauthorized access to Personal Data, where the impact level is significantly high, the Controller shall immediately notify the Data Subject of the following:

   a. The nature of the incident and the type of the Personal Data Subject's Personal Data that has been breached, damaged or accessed in an unauthorized manner; in clear and express language.

   b. The potential risks that may result from the incident, and the steps that have been taken to avoid or mitigate the adverse effects.

   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. Opinion and advice to help the Data Subject take appropriate action to avoid potential risks or mitigate their adverse effects.

2. The level of impact is deemed significantly high if it could result in serious damage (physical or moral) that is difficult to rectify or repair in the short term, and may extend to the family or relatives of the Data Subject or extent further to a certain group of the society, including:

    a. Bodily harm, such as stalking and assault, in the event of Data Breach of the location data indicating the movements of the Data Subject.

    b. Economic or financial damage, such as property loss or damage or unexpected financial loss, in the event of Data breach of credit card data of the Personal Data Subject or data related to the pattern of power consumption at home.

    c. Mental or psychological damage such as constant worry and fear of surveillance, unfair treatment and misuse of Personal Data, in the event of Data Breach of Personal Data related to lifestyle and health condition, which may lead to discrimination in making decisions relating to employment or insurance.

    d. Damage to reputation and dignity, such as embarrassment and humiliation, in the event of Data Breach of Personal Data related to intellectual views or personal preferences concerning controversial topics that are not socially accepted.

Article 25 - Restrictions on Disclosure of Personal Data

1. When disclosing Personal Data, the Controller shall observe the following:

    a. The request shall be written, justified and concerning a specific matter.

    b. The request shall be limited to the minimum required data.

    c. The entity to which the disclosure is made shall comply with the requirements of the Law and regulations during the processing.

2. If the disclosure is made to a Public Entity by a summons, court order, search warrant or any other legal procedure, the Controller shall, before disclosing the Personal Data, exercise the required care in a reasonable manner to notify the Data Subject, unless there is a legal restriction on such notification or unless such notification could adversely affect the integrity of the procedures of the Public Entity.

3. The Controller shall keep records of the disclosure that the Controller makes. Such records shall include the dates, methods, and purposes of the disclosure.

Article 26 - Disclosing Data of Person Other Than Data Subject

1. Before disclosing Personal Data linked to data of a person other than the Personal Data Subject, the Controller shall take into account the related circumstances, including:

    a. The type of Personal Data to be disclosed and the context of the processing of such data.

    b. Any confidentiality obligation concerning the data of the other person.

c. Striking a balance between the rights of the Personal Data Subject and the rights of the other person, in each case separately.

d. Whether it is possible to reach the other person to obtain their consent.

2. When disclosing Personal Data linked to data of a person other than the Data Subject, the Controller shall exercise due care and provide adequate guarantees to preserve the privacy of the other person and to ensure that such privacy is not violated, including to take the following steps:

   a. Delete or block the Personal Data that directly or indirectly indicates the identity of the other person.

   b. Obtain the consent of the other person, after assessing the potential risks and adverse effects that may result from the other person's becoming aware of the disclosure request, taking into account that such other person was not aware that their own data are linked to the Personal Data of the Data Subject, and consider whether it is appropriate if such other person becomes aware of such facts.

3. In the following cases, the Controller may disclose the data of another person if such data is generally known to the Personal Data Subject or the entity that requested the disclosure:

   a. If the entity requesting the disclosure has previously received the data of the other person (in previous activities).

   b. If the data of the other person is publicly available.

   Publicly available data means Personal Data that is legitimately published to the public.

Chapter VI: General Provisions on Impact Assessment of Processing

Article 27 - Assessment of Potential Impact and Risk

1. Impact assessment of processing of Personal Data in relation to any product or service provided to the public which may adversely affect the privacy of Personal Data Subjects shall be carried out in accordance with a form prepared by the Controller for that purpose. The Processor, if any, shall be provided with a copy of the said form. The form shall be subject to regular review to ensure that it fulfills its purpose. The impact assessment form shall:

   a. 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.

   b. Describe the scope of the processing by identifying the target group and the geographical scope.

   c. Describe the context of the processing by identifying the relation between the Personal Data Subject and the processor, and all the surrounding circumstances.

d. 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.

e. Identify the legal justification and Practical Need of the processing.

f. Identify and assess risks based on their probability and the severity of the physical and moral impact of those risks, such as psychological, social, bodily or financial impact.

g. Identify measures and solutions to mitigate risks.

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

2. The Controller shall conduct impact assessment in each of the following cases:

   a. Collection and processing of Sensitive Data, or data relating to those who are partially or completely legally incompetent or relating to Special Categories.

   b. Collection and processing of data using emerging technological means.

   c. Collection or comparing of data from different sources.

   d. Collection and analyzing of a set of data —related a person— from different sources, for the purpose of Profiling specific categories of people.

   e. Conducting activities relating monitoring or tracking technologies.

3. The Controller shall submit to the top official of the Controller, or the delegate authorized by such top official, the results of the impact assessment for each case, in the form referred to in paragraph 1 of this Article. Based on the said results, the official shall determine the level of the risks, their acceptability, to what extent their probability can be reduced and the severity of their impact, and shall accordingly decide whether to continue or stop the processing.

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 Controller 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 Controller. The Regulatory Authority may consult the Competent Authority in that respect.

Chapter VII: Transfer or Disclosure of Personal Data to Parties outside the Kingdom

Article 28 - Transfer of Personal Data to outside the Kingdom

1. The Controller shall store and process Personal Data within the geographical boundaries of the Kingdom. Personal Data may not be stored or processed outside the Kingdom before conducting an impact assessment and obtaining the written approval of the Regulatory Authority after the Regulatory Authority has liaised with the Competent Authority on a base-by-case basis.

2. In addition to the purposes stated in Article 29 of the Law, Personal Data may be transferred to outside the Kingdom for the following purposes:

   a. Providing services directly to individuals if providing such services requires the transfer of Personal Data to outside the Kingdom, in a manner that is not contrary to the expectations of the individuals, and provided such individuals have given their consent in accordance with the consent procedures stated in this Regulation.

   b. Purposes relating to the public interest.

3. Except where it is extremely necessary to save the Data Subject's life outside the Kingdom or preserve the Data Subject's vital interests, or avoid, examine or treat an infection, the Controller shall apply to the Competent Authority before transferring or disclosing Personal Data to any entity outside the Kingdom, in accordance with Article 29 of the Law. The said application shall not be valid unless the following conditions are satisfied:

   a. The application shall be made at least 30 days before the date proposed for starting the transfer of the data to outside the Kingdom.

   b. The application shall include the following:

      (1) The Controller's name, address and registration number; and the country to which the data is to be transferred and in which the party to which the data is to be disclosed is located.

      (2) The purpose(s) of transferring the data to outside the Kingdom or the purpose(s) of disclosing the data.

      (3) The legal grounds based on which the data is to be transferred to outside the Kingdom or disclosed.

      (4) Categories description of the Personal Data Subjects and their Personal Data or the categories of the Personal Data belonging to such Personal Data Subjects

      (5) The entities to which the Personal Data is to be transferred or disclosed.

   c. The Competent Authority shall examine all the applications within 30 days of receiving each application. The Competent Authority may extend that period, including where the Competent Authority requests additional information from the Controller.

Article 29 - Criteria and Guarantees for Personal Data Transfer to a Country not on the Approval List

When transferring Personal Data to a country that is not on the approval list referred to in Article 30 of this Regulation, the Controller shall:

1. Conduct potential risk and impact assessment of each case separately. The assessment shall take into consideration whether the Controller or Processor located outside the

Kingdom (i.e. the recipient) would provide a sufficient level of protection to the rights of the Data Subjects, according to the following criteria:

a. General Criteria of Assessment

When assessing the level of protection of Personal Data, the Controller shall take into account the type, value, volume and sensitivity of the data to be transferred; the purpose of processing; the category of the target Data Subjects; the scope of the processing; the entities with which the data is to be shared; whether the processing will take place in a restricted or incidental manner, i.e. only for one time or a limited period, or repeatedly and regularly; the country from which the data has been collected; the stages of transfer of the data, which may pass through multiple countries; assessment of the level of Personal Data protection systems at the final destination country; and the administrative procedures and technological measures for protection of Personal Data. If the protection assessment results, based on the foregoing criteria, show high risks to the rights of Personal Data Subjects, the Controller shall conduct an impact assessment based on the special criteria.

b. Special Criteria of Assessment:

The Controller, when assessing the country to which the data is sought to be transferred in terms of such country's laws and regulations that protect the rights of Data Subjects in relation to processing of their Personal Data; adopting of international principles and standards for protection of Personal Data; adopting of codes of conduct, general practices or special standards for protection of Personal Data; or being a party to international agreements or obligations.

2. Provide appropriate safeguards to protect Personal Data and the rights of Personal Data Subjects, as follows:

   a. State in contracts and agreements standard clauses, approved by the Competent Authority, to restrict the transfer of Personal Data outside the Kingdom.

   b. If the Controller or the Processor operates within a multinational group, prepare binding internal common rules to apply to Personal Data transfers outside the Kingdom. Such rules shall be approved by the Competent Authority. The rules shall be incorporated as an appendix to contracts or service level agreements between the two parties. The consent of the Regulatory Authority shall be required if there is any other obligation binding on that Controller or Processor, or any of their respective affiliates in another country, that is likely to have an adverse effect on the safeguards provided by the binding common rules.

   c. Follow the rules set out in the Codes of Conduct approved by the Regulatory Authorities or the Competent Authority as an effective tool that defines the obligations of Controllers.

d. Where necessary, use independent third parties to issue accreditation certificates confirming the existence of appropriate safeguards provided by external Controllers or Processors.

e. Public Entities, being Controllers or Processors, shall sign a binding agreement for transfer of Personal Data. Such agreement shall include binding contractual provisions that ensure privacy of Data Subjects and protect their rights.

Article 30 - Adequacy List

The Competent Authority shall prepare a list of the countries that provide adequate level of protection for Personal Data and the rights of Data Subjects, provided such list shall be regularly updated based on the detected changes that affect the protection of Personal Data or the rights of Data Subjects, based on the following criteria:

1. Existence of appropriate regulations and legislation related to protection of Personal Data and the rights of Data Subjects; and the country is a party to appropriate international agreements and obligations.
2. The country has a supervisory authority to ensure compliance with laws and legislation mentioned above.

Article 31 – Exception for Kingdom's Government Entities Abroad

Transfer of Personal Data to entities abroad affiliated with the government of the Kingdom shall not be subject to the provisions of Article 28 and Article 29 of this Regulation. The Competent Authority shall, in coordination with the related authorities, prepare rules for that purpose that take into account the provision of adequate protection for Personal Data, while achieving the interest sought from the transfer of data.

Chapter VIII: Personal Data Protection Officer

Article 32 – The Need to Appoint Personal Data Protection Officer

Without prejudice to any applicable regulations, the Controller shall appoint one or more of its employees to be responsible for the Controller's obligations to implement the provisions of the Law and regulations, based on such needs as decided in the discretion of the Competent Authority. Such employee shall be titled "personal data protection officer". The Competent Authority shall assess the need to appoint a personal data protection officer based on a number of elements in the provisions of appointing the personal data protection officer.

Article 33 - Role of Personal Data Protection Officer

Controller's personal data protection officer shall follow up the implementation of the Law and regulations, monitor and supervise the procedures applicable at the Controller, and receive requests related to Personal Data in accordance with the provisions of this Law; and in particular:

1. Act as a direct point of contact with the Competent Authority and carry out the Competent Authority's decisions and instructions in relation to implementing the provisions of the Law and regulations.
2. Provide support and advice to help the Controller observe the provisions of the Law and regulations.
3. Supervise the impact assessment procedures and the review and audit reports relating to Personal Data protection rules, and document the assessment results and issue the recommendations necessary to implement them.
4. Enable the Personal Data Subject to exercise their rights under the Law.
5. Notify the Competent Authority in accordance with Article 20 of the Law.
6. Respond to the requests made by the Personal Data Subject or their representative, and respond to the Competent Authority in relation to the complaints made in accordance with the Law.
7. Follow up the recording and updating of the Controller's records of Personal Data activities and the record of the processing activities.
8. Deal with violations related to Personal Data at the Controller, and take corrective action in relation thereto.
9. Organize training programs for the Controller's employees as necessary to qualify them according to the requirements of the Law.

Chapter IX: General Provisions

Article 34 - Keeping Personal Data after Anonymization of Data Subject

When removing all that leads to specifically identifying the Personal Data Subject in order to keep such Personal Data after the purpose relating to such Personal Data has ended, the Controller shall comply with the controls and procedures set out in Article 14 of this Regulation.

Article 35 - Period of Keeping Records of Personal Data Processing

The Controller shall keep a record of the Personal Data processing activities for five years or until the purpose of collection of such Personal Data ends, whichever period is longer.

Article 36 - Registration in Competent Authority's Portal

The Competent Authority shall prepare a regulation for the portal referred to in paragraph 1 of Article 32 of the Law. Such regulation shall identify the portal work mechanism, the criteria, procedures and conditions of registration in the portal and the related fees according to the nature of the Controller's business and according to such classifications as the Competent Authority may set in this regard.

Article 37 - Licenses to Practicing Activities Related to Personal Data Protection

The Competent Authority shall prepare a regulation for licensing commercial, professional and non-profit activities related to the protection of Personal Data or activities related to the issuance of accreditation certificates. The regulation shall set out the conditions and procedures for granting such licenses, their duration and cancellation rules, the criteria for issuing accreditation certificates and the conditions for licensing a representative of a Controller outside the Kingdom that processes Personal Data of residents of the Kingdom.

Article 38 - Complaints and Reports

1. Personal Data Subject may make a complaint to the Competent Authority. Such complaint shall be made no later than 60 days from the date of the incident in question or 60 days from the date of the Personal Data Subject becoming aware of the incident.
2. The Competent Authority shall receive complaints and communications according to procedures that ensure speedy and quality dealing with such complaints and communications.
3. The Competent Authority shall record the complaints and communications against suspected violators of the Law in a register prepared for that purpose. Such register shall guarantee anonymity of submitters.
4. A complaint or communication shall include the following information:
    a. The place and time of the violation.
    b. The name, ID, address and telephone number of the submitter.
    c. Data of the suspected party.
    d. A clear and specific description of the violation, and the evidence and information accompanying the complaint or communication.
    e. Any such other requirements as the Competent Authority may decide.
5. The Competent Authority may refer the complaint or communication to the Regulatory Authority of the Controller, in which case the Regulatory Authority shall follow up the Controllers' handling of the complaint or communication.
6. The Regulatory Authority shall inform the Competent Authority —regularly as the Competent Authority may request— of the action taken in response to the complaints and communications referred to the Regulatory Authority.
7. The Competent Authority or the Regulatory Authority, as the case may be, shall examine the complaints and communications and their documents and evidence. The Competent Authority may contact the submitter as needed to request evidence or information.
8. The Competent Authority or the Regulatory Authority, as the case may be, shall take the necessary steps regarding the complaints and communications it receives, and shall notify

the submitter of the outcome reached by the Competent Authority. The Competent Authority may for that purpose seek assistance from any party as needed.

Article 39 - Competences of Violation Detection Officers

1. In order to carry out the violation detection duties, the employees and workers referred to in Article 37 of the Law shall have the following powers:
    a. Make supervisory visits to the suspected entities and their offices and branches, and document the visits in a report signed by the officer and the entity's representative. In the event that the entity has no representative or the representative refuses to sign the report, that shall be recorded in the report.
    b. Correspond with the Controller to request information or any related documents required to examine the violation. If the Controller fails to respond, that shall be recorded in a report.
    c. Communicate with the data protection officer to request information or any related documents required to examine the violation. If the data protection officer fails to respond, that shall be recorded in a report.
    d. Inspect, and obtain copies of, the records, data and documents held at the suspected entities.
    e. Identify and take possession of the means and tools used in committing the violation, document them in a report, and seize them with the Competent Authority until the violation incident is decided.
    f. Record the statement of the entity's representative or any person who has information that may help in detection of violations, and make a report of any such statement.
    g. Seek assistance of security authorities when needed.
2. The aforementioned employees and workers shall provide proof of their capacity on carrying out the activities relating to detection of the acts and violations stated in the Law and regulations.
3. The Competent Authority shall issue the code of ethics of the supervisory work. The aforementioned employees and workers shall observe the provisions of such code of ethics.