SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

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.
3. **Personal Data Breach:** Any incident that leads to the Disclosure, Destruction, or unauthorized access to Personal Data, whether intentional or accidental, and by any means, whether automated or manual.
4. **Vital Interest:** Any interest necessary to preserve the life of a Data Subject.
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, provided it does not adversely affect the rights and interests of the data subject.
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. Such additional data or information should be kept separately, and appropriate technical and administrative controls should be implemented to ensure that they are not specifically linked to data subject's identity.
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. **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 its Regulations shall not apply to an individual Processing Personal Data for purposes not exceeding 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: General provisions for Data Subject Rights

1- 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 period not exceeding (30) days and without delay. This period may be extended in case the implementation requires disproportionate effort, or if the Controller receives multiple requests from the data subject, provided that the extension period does not exceed an additional (30) days and the Data Subject is notified in advance of the extension with the reasons for the delay.
   b) Take the necessary technical, administrative, and organizational measures to ensure a prompt response to requests related to exercising rights.
   c) Take appropriate measures to verify the identity of the requester before executing the request in accordance with relevant legal requirements.
   d) Take the necessary measures to document and keep record of all received requests 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 4: Right to be informed

1- If the Personal Data is collected directly from the Data Subject, the Controller shall, before or when collecting the 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 Data.
   d) The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.
   e) Explanation about Data Subject'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- Paragraph (1) of this article shall not apply if the information specified in sub-paragraphs (a) to (g) is already available to the Data Subject, or if providing such information conflicts with any of the existing laws in the Kingdom.

3- If Personal Data is collected from a party other than the Data Subject, the Controller shall, without undue delay and within a period not exceeding (30) days, take necessary steps to provide to the Data Subject information specified in paragraph (1) of this article, in addition to the categories of Personal Data being processed and the source from which the Controller obtained it.

4- Paragraph (3) of this article shall not apply in any of the following conditions if:
   a) The information is already available to the Data Subject.
   b) the provision of such information proves impossible or would involve a disproportionate effort.
   c) The Controller collects data to fulfil a legal requirement.
   d) The Controller is a Public Entity and the Collection of Personal Data is for security purposes, or to fulfil judicial requirements, or to achieve a Public Interest.
   e) The Personal Data is subject to an obligation to a professional secrecy regulated by a law.

5- A Controller whose activities require continuous or large scale Processing of Personal Data on individuals lacking full or partial legal capacity or whose parents are unknown, 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 solely on automated Processing of Personal Data.

6- When the Controller engages in an additional Processing of Personal Data for a purpose other than the one for which it was initially collected for, it shall provide the Data Subject with the necessary information in accordance with the provisions of this article, before conducting such additional Processing.

7- The Controller shall provide the required information in an appropriate language as stipulated in this Article when aware that the Data Subject lacks full or partial legal capacity.

Article 5: Right of access to Personal Data

1- Without prejudice to the provisions of Articles (9) and (16) of the Law, the Data Subject shall have the right to access their Personal Data at the disposal of the Controller, subject to the following:

a) Exercising the right to access Personal Data shall not adversely affect the rights of others, such as intellectual property rights or trade secrets.
b) Accessing to Personal Data at a request from the Data Subject, or via a channel provided by the Controller to the Data Subject allowing direct access to their Personal Data without the need to make a request.

2- When granting the Data Subject access their Personal Data, the Controller shall ensure that no Personal Data identifying another individual is not disclosed.

Article 6: Right to Request Access to Personal Data

Subject to the provisions of Article (4) of the Law, the Data Subject shall have the right to request a copy of their Personal Data in a readable and clear format, subject to the following:

1- Exercising the right to access Personal Data shall not adversely affect the rights of others, such as intellectual property rights or trade secrets.
2- Personal Data shall be provided to the Data Subject in a commonly used electronic format and the Data Subject may request a printed hard copy if feasible.
3- When granting a Data Subject access to their Personal Data, the Controller shall ensure that it does not involve disclosing Personal Data that identifies another individual.

Article 7: Right to Request Correction of Personal Data

1- Data Subject shall have the right to obtain from the Controller a 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 this Regulation.

2- 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 once the verification process is completed.

3- Upon correcting Personal Data, the Controller shall notify without undue delay the parties to whom Personal Data have been previously disclosed.

Article 8: Right to Request Destruction of Personal Data

1- The Controller shall destroy Personal Data in any of the following cases:
   a) Upon Data Subject's request.
   b) If the Personal Data are no longer necessary to achieve the purpose for which they were collected.
   c) If the Data Subject withdraws their consent, and consent is the sole legal basis for Processing.
   d) If the Controller becomes aware that the Personal Data have been unlawfully processed.

2- When destroying Personal Data, the Controller shall take the following steps:
   a) Take appropriate measures to notify other parties to whom the Controller has disclosed such Personal Data and request their Destruction.
   b) Take the appropriate measures to notify the individuals to whom the Personal Data have been disclosed by any means and request their Destruction.
   c) Destroy all copies of the Personal Data stored in the Controller's systems, including backups, in accordance with relevant regulatory requirements.

3- The provisions of this article shall not prejudice the requirements specified in Article 18 of the Law and the legal requirements established by the relevant Competent Authorities.

Article 9: Anonymisation

1- When a Controller anonymizes the Personal Data of a Data Subject, it shall comply with the following:
   a) Ensure that re-identification of the Data Subject is impossible after Anonymisation.
   b) Evaluate the impact, including the possibility of re-identifying the Data Subject, in the circumstances specified in Paragraph (1) of Article 25 of this Regulation.
   c) Take the necessary organizational, administrative, and technical measures to avoid risks, taking into account technological developments and methods of Anonymisation, and update those methods considering such developments.
   d) Evaluate the effectiveness of the applied techniques for Personal Data Anonymization and make necessary adjustments to ensure that re-identification of Data Subject is impossible.
2- Anonymized data shall no longer be considered as Personal Data.

Article 10: 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 lawful communication mean provided by the Controller for this purpose.

Article 11: Consent

1- The Controller shall obtain Data Subject's consent to Process their Data in any appropriate form or means, including written or verbal consent or electronic means, subject to the following conditions:
   a) 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) Processing purposes shall be clear, specific, and shall be explained and clarified to the Data Subject before or at the time of requesting consent.
   c) Consent shall be given by a person who has full legal capacity.
   d) Consent shall be documented through means allowing future verification, such as keeping registers recording Data Subjects' consent for Processing operations, specifying time and the mean of Consent.

e) A separate consent shall be obtained for each Processing purpose.

2- Data Subject's consent shall be explicit in the following cases:
   a) When the Processing involves Sensitive Data.
   b) When the Processing involves Credit Data.
   c) When decisions are made solely based on automated Processing of Personal Data.

Article 12: Consent withdrawal

1- A Data Subject shall have 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 mean in accordance with Article (4) of this Regulation.

2- Before requesting consent from the Data Subject, the Controller shall establish procedures that allow for the withdrawal of such consent and take the necessary measures to ensure their implementation, ensuring that consent withdrawal is as or easier than obtaining.

3- In the event of consent withdrawal, the Controller shall cease Processing without undue delay from consent withdrawal request. Consent withdrawal of 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.

5- Consent withdrawal shall not affect the Processing of Personal Data that is based on another legal bases.

Article 13: Legal Guardian

1- Considering applicable legal requirements, the legal guardian of a Data Subject that lacks full or partial 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 this Regulation.
   b) Consent to the Processing of the Data Subject's Personal Data in accordance with the provisions of the Law and this Regulation.

2- In addition to what is stipulated in paragraph (1) of Article 11 of this Regulations, in case of Processing Personal Data of a Data Subject that lack full or partial legal capacity, obtaining the consent of the legal guardian shall be conditioned upon taking appropriate measures to verify guardianship validity over the Data Subject.

3- When obtaining the consent from the legal guardian of a Data Subject that lacks full or partial legal capacity, the Controller shall comply with the following provisions:
   a) Consent given by legal guardian shall not cause any harm to the interests of the Data Subject.
   b) The Data Subject shall be allowed to exercise their rights stipulated in the Law and this Regulation when they reach legal capacity.

Article 14: Processing to serve Actual Interest of Data Subject

When processing data to serve Actual Interest of the Data Subject, the Controller shall retain evidence that such interest exists and that it is not possible to contact or communicate with the Data Subject.

Article 15: Collecting Data from Third Parties

1- Except for 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) Processing is necessary and proportionate to the specified purpose.
   b) Processing 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 (9) of this Regulation regarding Anonymisation.

Article 16: Processing for Legitimate Interest

1- Except Public Entities, a Controller may process Personal Data to achieve a Legitimate Interest provided that the following conditions are met:
   a) Purpose shall not violate any of the laws in the Kingdom.

b) The rights and interests of the Data Subject and the Legitimate Interest of the Controller shall be balanced, so that the interests of the Controller do not affect the rights and interests of the Data Subject.
c) Processing shall not include Sensitive Data.
d) Processing shall be within the reasonable expectations of the Data Subject.

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 that 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) Evaluation of whether the proposed Processing will cause any potential harm to Data Subjects or their ability to exercise their legally established rights.
e) Identification of any measures that shall be taken to avoid potential risks or harms, in accordance with the provisions of paragraph (2) of Article (25) of this Regulation.

4- If the assessment outlined in paragraph (3) of this article indicates that the proposed Processing will in any way violate any law, 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, or consider relying on another legal basis.

Article 17: Processor selection

1- The Controller shall ensure that any Processor selected provides sufficient guarantees to protect Personal Data, and that the agreement with the Processor includes the following:
   a) Purpose of the Processing.
   b) Categories of Personal Data being processed.
   c) Duration of the Processing.
   d) Processor's commitment to notify, without undue delay, the Controller in case of a Personal Data Breach occurs, in accordance with the provisions of the Lawthis Regulation.
   e) Clarification of whether the Processor is subject to Regulations in other countries and the impact on their compliance with the Law and its Regulations.
   f) Not requiring the Data Subject's prior consent for mandatory Disclosure of Personal Data under the applicable laws in the Kingdom, provided that the Processor notifies the Controller of such Disclosure.
   g) Identifying any subcontractors contracted by the 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 to periodically assess Processor's compliance with the Law and its Regulations, and ensuring that all regulatory requirements are met, whether the Processing is achieved by the Processor or third parties acting under their behalf. The 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 Processor shall be considered as a Controller and held directly accountable for any violation of any provisions of the Law.

5- Before entering any subsequent contracts with sub-Processors, the Processor shall abide by the following:
   a) Take sufficient guarantees to ensure that such contracts would not impact the level of protection provided to the Personal Data being processed.

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

c) Obtain prior acceptance from 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 Processor.

Article 18: Processing data for a purpose other than the one for which it was collected

1- When the Controller Processes Personal Data for a purpose other than the one for which it was initially collected as provided in Article 10 of the Law, it shall do the following:

a) Define clearly and specifically the Processing purposes.

b) Document the procedures to fix 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) 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- Except for cases stated in paragraph (3) of Article 10 of the Law, when the Controller Processes Personal Data for a purpose other than the one for which it was initially collected as provided in paragraphs (1), (2), (4), (5), and (6) of Article 10 of the Law, the Controller shall comply with the following:

a) Define clearly and accurately 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 19: 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, and this shall be determined using appropriate means, including 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.

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

Article 20: Disclosure of Personal Data

1- Disclosure of data collected from publicly available sources under paragraph (2) of Article 15 of the Law is allowed under the condition that such data have not been made available to the public in violation of the provisions of the Law and its Regulations.

2- Except for the circumstances provided 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 fulfil requirements of another law, or to fulfil judicial requirements, or if the disclosure is necessary to protect public health or public safety, or to protect the life of specific individuals' or their health, the following measures shall be taken:
   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 considering the following steps:

a) In each separate case, balancing between the rights of the Data Subject and the rights of the other person.
b) Whenever possible, pseudonymisation of Personal Data allowing the identification of the other person.

5. When disclosing Personal Data to achieve a Legitimate Interest for the Controller, the Controller shall comply with the provisions of Article 16 of this Regulation.

6. The Controller shall include Disclosure operations in the records of Personal Data Processing activities, document the dates, methods, and purposes of Disclosure.

Article 21: 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 a purpose other than the one for which it was initially collected, or requests Disclosure of such data to achieve a public interest, the Public Entity shall comply with the following:

a) Ensure that this is necessary to achieve a clearly defined public interest.
b) The public interest related to Public Entity's mandate as specified in the regulation.
c) Take suitable measures to limit the damage that may result, including implementing necessary administrative and technical controls to ensure its agents commit to comply with the provisions of Article 41 of the Law.
d) Record those operations in the records of Personal Data Processing activities.
e) Collect and Process the minimum necessary Personal Data to achieve data Processing purpose.

Article 22: 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 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 without undue delay.

5- The Controller shall take appropriate organizational, administrative and technical 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 this Regulation, including procedures that enable Data Subjects to exercise their right to request correction in accordance with the provisions of the Law and this Regulation.
   b) Periodic review of the accuracy and timeliness of Personal Data.

Article 23: Information Security

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

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

b) Adopt all relevant controls, standards, and rules issued by the National Cybersecurity Authority, or adopt recognized best practices and cybersecurity standards If the Controller is not obligated to follow the controls, standards, and rules issued by the National Cybersecurity Authority.

Article 24: 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) 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) Contact details of the Controller or its data protection officer, if any, or any other official having 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) Description of the Personal Data Breach.

b) 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) 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 25: Impact Assessment

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 Personal Data Processing. Impact assessment shall be conducted in the following cases:

a) Processing of Sensitive Data.

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

c) The activity of the Controller includes - large scale and repetitive - Processing of Personal Data of those who lack full or partial legal capacity, or processing operations that by their nature require constant monitoring of Data Subjects, or Processing Personal Data based on newly adopted technologies, or making decisions based on automated Personal Data Processing.

d) Providing a product or service that involves Processing Personal Data that is likely to cause serious harm to Data Subjects privacy.

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

a) Purpose of the Processing and its legal basis.

b) 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) Description of the scope of the Processing, which identifies the type of Personal Data and the geographical scope of the Processing.

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

e) Necessity and proportionality of the measures to be taken to enable the Controller and Processors to process the minimum Personal Data necessary to achieve the purposes of the Processing.

f) 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) Measures that to be taken to prevent or mitigate risks.

h) The suitability of planned measures to prevent identified risks.

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

4- If the impact assessment mentioned in this article indicates that a Processing operation it to harm Data Subjects privacy, the Controller shall address the causes of such harm and re-conduct an impact assessment.

Article 26: Processing Health Data

The Controller shall take the appropriate organizational, technical, and administrative measures to protect 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- Adopt the provisions of the Law and its Regulations into the internal policies of the Controller.

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 Data Subjects privacy.

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 Health Data Processing - shall include provisions that oblige them to abide by the procedures and measures stated in this Article.

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

Article 27: Processing Credit Data

Without prejudice to the provisions of the Credit Information Law, the Controller shall take organizational, technical, and administrative measures to protect 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 process Credit Data.

2- Controller shall obtain Data Subject consent and notify them of any request to disclose their Credit Data in accordance with the provisions of the Credit Information Law, while considering the provisions stated in subparagraph (d) of paragraph (1) of Article 11 of the Regulation.

Article 28: Processing Data for Advertising or Awareness Purposes

1- Controller shall obtain Consent from a targeted recipient before sending advertising or awareness material in case of the absence of a prior interaction between the Controller and the targeted recipient.

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

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

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

c) Consent of a targeted recipient shall be documented in a manner allowing future verification.

3- Without prejudice to the Telecommunication and Information Technology Act or any other related laws, before using communication methods for the purpose of sending

advertising or awareness material, including via postal and electronic addresses of the Data Subject, the Controller shall commit to the following:

a) Clearly mention sender's name without hiding their identity.
b) Provide a mechanism that enables the Data Subject to halt reception of advertising and awareness materials when desired, and ensure that the procedures to halt the of reception of such material are as simple and easy as the procedures to the obtain consent to receive the material.
c) Immediately halt sending advertising or awareness material upon request from targeted recipient.
d) Halting reception of advertising or awareness material shall be free of charge.
e) Keep material evidence of consent from the targeted recipient to receive advertising or awareness material.

Article 29: Direct Marketing

1- Without prejudice to the Telecommunication and Information Technology Act or any other related laws, before Processing Personal Data for Direct Marketing purposes, the Controller shall abide by to the following:
   a) Obtain consent from the Data Subject in accordance with the provisions of Article (11) of this Regulation.
   b) Provide a mechanism that enables the Data Subject to halt the reception of marketing material whenever desired, and ensure that the procedure for halting the reception such material are as simple and easy the procedure to obtain the consent to receive the material
2- When sending direct marketing material to a Data Subject, the identity of the sender shall be clearly disclosed.
3- When the Data Subject withdraws their consent for Direct Marketing purpose, the Controller shall halt without undue delay sending marketing material.

Article 30: Collection and Processing of Data for Scientific, Research, or Statistical Purposes

When collecting or Processing Personal Data for scientific, research, or statistical purposes without Data Subject's consent, the Controller shall commit to the following:

1- Clearly and accurately specify the scientific, research, or statistical purposes in the records of Personal Data Processing activities

2- Take the necessary measures to ensure that only the minimum Personal Data necessary to achieve the specified purposes is collected.

3- Pseudonymise Personal Data that is being processed, provided that those purposes of the processing can be fulfilled

4- 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 31: 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 fulfill a legal requirement. 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 32: 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 involving Processing of Personal Data on a large scale.

b) The controller's primary activities are based on processing operations that, by their nature, require regular and systematic monitoring of Data Subjects.

c) Core activities of the Controller are based on processing sensitive Personal Data.

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

3- The personal data protection officer is responsible for monitoring the implementation of the provisions of the Law and its Regulations, overseeing the procedures adopted by the Controller, and receiving requests related to Personal Data in accordance with the provisions of the Law and its Regulations. Specifically, their responsibilities include:

a) Acting as the direct point of contact with the Competent Authority and implementing its decisions and instructions regarding the application of the provisions of the Law and its Regulations.
b) Supervising impact assessment procedures, audit and control reporting related to Personal Data protection requirements, documenting assessment results, and issuing necessary recommendations.
c) Enabling the Data Subject to exercise their rights as stipulated in the Law.
d) Notifying the Competent Authority of Personal Data Breach incidents.
e) Responding to requests from Data Subjects and addressing complaints filed by them in accordance with the provisions of the Law and its Regulations
f) Monitoring and updating the records of personal data processing activities of the Controller.
g) Handling Controller's violations related to Personal Data and taking corrective actions accordingly.

4. 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.

Article 33: Records of Personal Data Processing Activities

1- The Controller shall keep a record of Personal Data Processing activities during all the period Personal Data is being processed, and till to five years after the date of end of any Personal Data Processing activity.
2- Records of Personal Data Processing activities shall be written.
3- Controller shall ensure that the records of Personal Data Processing activities are accurate and up to date.
4- Controller shall provide access to the records of Personal Data Processing activities to the Competent Authority upon request.
5- The record of Personal Data Processing activities shall include, at a minimum, the following:
    a) Controller's name and relevant contact details.
    b) Information about the Data Protection Officer, where required in accordance with Article (32) of this Regulation.
    c) Purposes of the Personal Data processing.
    d) Description of Personal Data categories being processed and Data Subjects categories.
    e) Retention periods for each Personal Data category, where possible.
    f) Categories of recipients to whom the Personal Data is disclosed.
    g) Description of operations of Personal Data Transfer outside the Kingdom, including the legal basis for the Transfer and recipient parties.
    h) Description of the procedures and organizational, administrative, and technical measures in place that ensure the security of Personal Data, where possible.
6- Competent Authority shall provide templates of records of Personal Data Processing activities.

Article 34: National Register of Controllers

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

Article 35: 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. The Competent Authority shall also coordinate with the Digital Government Authority regarding licensing for entities providing services on behalf of government entities.

Article 36: Auditing and Controlling

1- The purpose of auditing and controlling is to ensure that the entity is properly protecting Personal Data through audits and checks of Personal Data processing activities, and related controls and procedures, and identification of compliance gaps with the Law and its Regulations.

2- When carrying out audits or controls of Personal Data Processing activities, the following shall be respected:
   a) Providing services with independence according to applicable professional standards.
   b) Developing the necessary administrative and organizational procedures and controls to ensure the accuracy and integrity issued output.

3- The Competent Authority shall issue the rules for licensing entities that undertake auditing or checking of Personal Data Processing activities in accordance with paragraph (3) of Article 33 of the Law. The Competent Authority shall also coordinate with the Digital Government Authority regarding licensing for entities providing services on behalf of government entities.

Article 37: Submitting and processing complaints

1- A Data Subject may submit a complaint to the Competent Authority within a period not exceeding (90) days from the date when the incident occurred or when the Data Subject became aware of it. The Competent Authority shall decide about the admissibility of the complaint after aforementioned delay when there are reasonable

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

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

3- Competent Authority shall keep a record of the complaints filed in a register specifically created for this purpose.

4- The complaint shall include the following information:
   a) Place and time of the violation.
   b) Name, identification, address, and telephone number of the complainant.
   c) Information about the complained entity.
   d) 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 may communicate with the complainant 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.

Article 38: Publication and Enforcement

This 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.


SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority