SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

The Implementing Regulation of the Personal Data Protection Law

Translation for guidance, please refer to the Arabic version for the original text.

Index:

First:

Second:

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. The pseudonymised data or additional information should be kept separately, and appropriate technical and administrative controls should be implemented to ensure that they are not specifically linked to the data subject's identity.
8- **Anonymisation:** 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 of 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 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 submitted, including oral requests.

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

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

Article 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- The provisions of 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 directly from an individual other than the Data Subject, the Controller shall, without undue delay and within a period not exceeding (30)

days, take necessary steps to inform the Data Subject of the provisions 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- The provisions of 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 implementation is not possible or requires disproportionate effort.
c) The Controller obtained the data in accordance with a law.
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 professional confidentiality provisions established by law.

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

a) Means and methods of collecting and Processing Sensitive Data, where applicable.
b) Means and procedures taken to protect Personal Data.
c) Indicate whether decisions will be made based solely on automated Processing of Personal Data.

6- When the Controller engages in 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 the 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 fully or partially lacks 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 has the right to access their Personal Data available with the Controller, subject to the following:
   a) Exercising the right to access Personal Data should not negatively impact the rights of others, such as intellectual property rights or trade secrets.
   b) Providing access to Personal Data at a request from the Data Subject, or via a channel provided by the Controller enabling Data Subject to directly access their Personal Data without the need to make a request.
2- When enabling the Data Subject to access their Personal Data, the Controller shall ensure that it does not involve disclosing Personal Data that identifies another individual.

Article 6: Right to Request Access to Personal Data

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

1- Exercising the right to access Personal Data should not negatively impact the rights of others, such as intellectual property rights or trade secrets.
2- The Personal Data is 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 the Personal Data, the Controller shall notify the parties to whom the Personal Data was previously disclosed without delay.

Article 8: Right to Request Destruction of Personal Data

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

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

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 the 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 the risks, taking into account technological developments, methods of Anonymisation, and updates to those methods.
d) Evaluate the effectiveness of the applied techniques for anonymising Personal Data and make necessary adjustments to ensure that re-identification of Data Subject is impossible.

2- Anonymized data shall not 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 communication mean provided by the Controller for this purpose.

Article 11: Consent

1- The Controller shall obtain the Data Subject's consent for Processing their Data in any appropriate form or means, including written or verbal consent or by using electronic methods, 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 in a way that allows verification in the future, such as keeping records that include the Consent of the Data Subjects regarding the Processing operations, along with the time and the method of Consent.
e) Independent consent shall be obtained for each Processing purpose.

2- The 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- Data Subject has the right to withdraw their consent for Processing their Personal Data at any time, and they shall inform the Controller of this through any available means according to Article (4) of this Regulation.
2- Before requesting consent from the Data Subject, the Controller shall establish procedures that allow for the withdrawal of that consent and take the necessary measures to ensure their implementation, with the procedures for withdrawing consent being similar to or easier than those for obtaining it.
3- In the event of consent withdrawal, the Controller shall cease Processing without undue delay from withdrawal request. The withdrawal of consent shall not affect the lawfulness of Processing based on consent before its withdrawal.
4- When the Data Subject withdraws their consent for Processing their data, the Controller shall take appropriate measures to notify those to whom the Personal Data has been disclosed and request its Destruction through any available means.
5- Consent withdrawal shall not affect the Processing of Personal Data that is based on other legal basis.

Article 13: Legal Guardian

1- Considering applicable legal requirements, the legal guardian of the Data Subject that fully or partially lacks legal capacity shall act in the best interests of the Data Subject and for this purpose, they have the following options:
   a) Exercise the rights granted to the Data Subject under the Law and 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 fully or partially lacks legal capacity, obtaining the consent of the legal guardian is conditional upon taking appropriate measures to verify validity of guardianship over the Data Subject.

3- When obtaining the consent from the legal guardian of a Data Subject that fully or partially lacks legal capacity, the Controller shall comply with the following provisions:
   a) It shall not cause any harm to the interests of the Data Subject.
   b) It shall enable the Data Subject to exercise their rights as provided in the Law and this Regulation when they reach legal capacity.

Article 14: Processing to Serve the Actual Interest of Data Subject

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

Article 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 shall be 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 in cases where the Controller is a Public Entity, the 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) A balance between the rights and interests of the Data Subject and the Legitimate Interest of the Controller, 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 laws, infringe on the rights and interests of Data Subjects, cause harm to them or any other party, the Controller shall modify the proposed Processing and conduct a new assessment, or consider relying on another legal basis.

Article 17: Choosing the Processor

1- The Controller shall ensure that any Processor chosen 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 the Controller in case of a Personal Data Breach, in accordance with the provisions of the Law, this Regulation, and without undue delay.
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 violating 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: Further Processing of Personal Data

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) Clearly and specifically define 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.

1- 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) Clearly and accurately define the purpose of the Processing and refer to it in the records of Personal Data Processing activities.
b) Limit the Collection and Processing of the Personal Data to the minimum amount necessary to achieve the purpose.
c) Identify the type of Personal Data to be processed and the necessary measures to ensure that such data is processed appropriately.

Article 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 conditional upon ensuring that such Disclosure to the public has not been carried out 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 implement another law, or to satisfy legal requirements, or if the disclosure is necessary to protect public health, public safety, or to protect the life or specific individuals' 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) Balance between the rights of the Data Subject and the rights of any other person in each case separately.

b) Pseudonymisation of Personal Data that indicates the identity of another individual whenever possible.

5- When disclosing Personal Data to achieve a Legitimate Interest of 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:

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

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

3- Take suitable measures to limit the damage that may result, including implementing necessary administrative and technical controls to ensure its personnel's compliance with the provisions of Article 41 of the Law.

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

5- Collecting and Processing the minimum necessary Personal Data to achieve the 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 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 the security of Personal Data and the privacy of the Data Subjects, and shall comply with the following:

1- Implement necessary security and technical measures to limit security risks related to Personal Data Breach.

2- Comply with relevant controls, standards, and rules issued by the National Cybersecurity Authority or 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 sets of Personal Data obtained from different sources.
   c) The activity of the Controller includes - continuous and large scale - Processing of Personal Data of those who fully or partially lack legal capacity, or Processing operations that by their nature require continuous monitoring of Data Subjects, or Processing Personal Data using new technologies, or making decisions based on automated Processing of Personal Data.
   d) Providing a product or service that involves Processing Personal Data that is likely to cause serious harm to the privacy of Data Subjects.
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 context of the Processing, which identifies the relationship between the Data Subjects, the Controller, and the Processors, as well as any other relevant circumstances.
e) Necessity and proportionality of the measures to be taken to enable the Controller and Processors to process the minimal Personal Data necessary to achieve the purposes of the Processing.
f) 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 will be taken to prevent or limit the risks.
h) The suitability of the measures envisaged to avoid 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- The Controller shall - if the assessment mentioned in this article indicates that the Processing operation will harm the privacy of the Data Subjects - address the reasons for that and re-conduct the 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- Include 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 the privacy of the Data Subjects.
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 the consent of the Data Subject and notify them of any request to disclose their Credit Data in accordance with the provisions of the Credit Information Law, 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 the Consent from the 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 consent shall be documented in a manner that can be verified in the future.

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 materials, including the post and email 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 opt out of receiving advertising and awareness materials when desired, and ensure that the procedures for opting out of receiving such materials are easy, straightforward, and at least as easy as the procedures for giving consent to receive them.

   c) Stop sending advertising or awareness materials as soon as the target recipient requests it.

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

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

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 Data Subject in accordance with the provisions of Article (11) of this Regulation.

b) Provide a mechanism that enables the Data Subject to opt out of receiving marketing materials when desired, and ensure that the procedures for opting out of receiving such materials are easy, straightforward, and at least as easy as the procedures for giving consent to receive them.

2- When sending direct marketing materials to a Data Subject, the identity of the sending entity shall be clearly stated without any anonymisation.
3- In case the Data Subject withdraws their consent for Direct Marketing, the Controller shall immediately stop sending related marketing materials without undue delay.

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 minimal Personal Data necessary to achieve the specified purposes is collected.
3- Pseudonymise Personal Data that is being processed, in cases where this does not impact the achievement of the Processing purpose.
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 when required by Law. The Controller shall provide the necessary protection for such documents and

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

Article 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) Controller is a Public Entity that provides services involving Processing of Personal Data on a large scale.
   b) Primary activities of the Controller consist of Processing operations that require regular and continuous monitoring of individuals on a large scale.
   c) Core activities of the Controller consist of Processing sensitive Personal Data.
2- Subject to the requirements of paragraph (1) of this Article, the data protection officer may be an official, an employee or an external contractor of the Controller.
3- The 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 the impact assessment procedures, audit reports, and evaluations related to Personal Data protection controls, documenting the assessment results, and issuing necessary recommendations accordingly.
   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 the 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 retain the record of Personal Data Processing activities during the period of the Processing, in addition to five years starting from the date of completion of the 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 the categories of Personal Data being processed and the categories of Data Subjects.

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

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

g) Description of Personal Data Transfers outside the Kingdom, including the legal basis for the Transfers and the recipients of the Personal Data.

h) Description of the procedures and the 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

1- The purpose of audit and checking is to ensure that the entity is properly protecting Personal Data through auditing and checking of carried out Personal Data Processing activities, and related controls and procedures, and identifying any gaps in compliance with the Law and its Regulations.
2- When carrying out audit or checking of Personal Data Processing activities, entities shall adhere to the following:
   a) Provide the services independently according to professional standards.
   b) Develop the necessary administrative and organizational procedures and controls to ensure the accuracy and integrity of their output.
3- The Competent Authority shall issue the rules for licensing entities that undertake auditing or 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: Filing and Processing Complaints

1- Data Subject may complain to the Competent Authority within a period not exceeding (90) days from the date of the incident or the date on which the Data Subject became aware of it. The Competent Authority shall determine whether to accept the complaint or not after this period in cases where there are reasonable causes that may have prevented the Data Subject from submitting the complaint in time.
2- Competent Authority shall receive the complaints that are submitted to it, through the designated means 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

Regulation on Personal Data Transfer outside the Kingdom

Chapter 1: Definitions and General Provisions

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 9/2/1443 AH and amended by Royal Decree No. (M/148) dated 5/9/1444 AH and its implementing Regulations. 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 for the Personal Data Transfer outside the Kingdom.
2- **Transfer of Personal Data**: The Transfer of Personal Data outside the Kingdom for the purpose of processing.
3- **Regulations**: The implementing Regulations of the Personal Data Protection Law.

Article 2: General Provisions for the Transfer of Personal Data outside the Kingdom

1- Subject to the provisions of the Law and its Regulations, a Controller may Transfer Personal Data or disclose it to a party outside the Kingdom, provided that such Transfer or Disclosure does not impact national security or vital Interests of the Kingdom or violate any other law in the Kingdom.
2- The Controller shall limit the Transfer or Disclosure of Personal Data outside the Kingdom to a party outside the Kingdom to the minimum necessary to achieve the purpose of the Transfer or Disclosure through the use of any appropriate mean including data maps that indicate the need to Transfer or disclose each data and link it to one of the purposes for processing outside the Kingdom.
3- When transferring or disclosing Personal Data to a party outside the Kingdom, the Controller shall ensure that such Transfer or Disclosure does not impact the privacy of Data Subjects or the level of protection guaranteed for Personal Data under the Law and its Regulations, by ensuring that the Transfer or Disclosure will not compromise -at least- any of the following:
   a) Data Subject's ability to exercise their rights guaranteed by the Law.
   b) Data Subject's ability to withdraw their consent to the processing.
   c) Controller's ability to comply with requirements for notifying Personal Data Breaches.
   d) Controller's ability to comply with provisions, controls, and procedures for disclosing Personal Data.

e) Controller's ability to comply with provisions and controls for destroying Personal Data.
f) Controller's ability to take necessary organizational, administrative, and technical measures to ensure the security of Personal Data.

4- The Controller may transfer personal data outside the Kingdom or disclose it to a party outside the Kingdom for any of with the purposes stipulated in paragraph (1) of Article (29) of the Law, or any to the following purposes:
a) If conducting processing operations enables the Controller to carry out its activities, including central management operations.
b) If that results in providing a service or benefit to the personal data subject.
c) If this is to conduct scientific research and studies

Chapter 2: Transfer based on adequate level of protection for Personal Data

Article 3: Evaluation of the Level of Protection for Personal Data

1- The Competent Authority and the concerned authorities with which it coordinates - each according to its jurisdiction - shall evaluate the level of protection for Personal Data outside the Kingdom in accordance with the following criteria:
a) Existence of laws that ensure the protection for Personal Data and preserve the rights of Data Subjects, at a level of protection that is not less than the guaranteed by the Law and its Regulations.
b) Rule of law to ensure the rights of Data Subjects and to preserve their privacy.
c) Effectiveness of the implementation of the Personal Data protection Laws.
d) Ability of Data Subjects to exercise their rights and the availability of the necessary means to file complaints or claims related to the processing of Personal Data.
e) Existence of a supervisory authority responsible for monitoring the compliance of controllers with Personal Data protection requirements.
f) Willingness of the data protection authority to cooperate with the Competent Authority of the Kingdom in matters related to Personal Data protection.
g) Clarity and appropriateness of regulatory requirements in regard to Disclosure of personal data to governmental or supervisory authorities.

2- The assessment of the level of protection for Personal Data referred to in this Article may be conducted for countries, specific sectors, or international organizations.

Article 4: Results of the Evaluation of the Personal Data Protection Level

1- The Competent Authority shall submit the results of the assessment of the level of protection for Personal Data outside the Kingdom to the Prime Minister, including all details related to it, such as the judgments of the participating authorities in the assessment and the recommendations of the Competent Authority.
2- The recommendations of the Competent Authority referred to in paragraph (1) of this Article shall be of the following:
   a) Recommending the issuance of an adequacy decision based on the results of the assessment of the level of Personal Data protection, whether all or some of the criteria stipulated in paragraph (1) of Article (3) of this Regulation have been met.
   b) Recommending the performance of an international agreement - in accordance with the applicable procedures.
   c) Recommending not to issue an adequacy decision or perform an international agreement, with a statement of the reasons for such a recommendation.
3- The Competent Authority shall - every four years or when necessary - review the assessment of the level of protection of Personal Data in countries, sectors or international organizations for which adequacy decisions have been issued or an international agreement has been signed, considering all relevant developments in those countries, sectors, or international organizations, in accordance with the criteria mentioned in paragraph (1) of Article (3) of this Regulation.
4- The Competent Authority shall propose to the Prime Minister the termination, amendment, or suspension of any decision taken regarding the level of protection for Personal Data outside the Kingdom if upon the review of the level of protection for Personal Data reveals that the country, sector, or international organization no longer guarantees an adequate level of protection for Personal Data.

Chapter 3: Exemption cases

Article 5: Transfer based on appropriate safeguards for transferring personal data outside the Kingdom

1- In the absence of an adequate level of protection for Personal Data outside the Kingdom, the Controller may transfer or disclose personal data outside the Kingdom, provided that the regulatory requirements in the country or the international organization do not bring any prejudice to the privacy of personal data subjects or the ability to enforce appropriate safeguards: The appropriate safeguard may be any of the following :

a) Binding Common Rules that apply to all parties involved in entities engaged in a joint economic activity, including their employees. These rules shall be approved by the Competent Authority in accordance with requests submitted to it in each case separately.
b) Standard Contractual Clauses that ensure a sufficient level of protection for Personal Data when transferred outside the Kingdom, in accordance with a standard model issued by the Competent Authority.
c) Certifications of compliance with the Law and its Regulations in the Kingdom, issued by an authorized entity by the Competent Authority, together with the enforceable commitments the Controller or Processor in the third country to apply the appropriate safeguards..
d) Binding Codes of Conduct, which are approved by the Competent Authority based on the requests submitted in each case separately, together with the enforceable commitments the Controller or Processor in the third country to apply the appropriate safeguards.

2- The Binding Common Rules referred to in subparagraph (A) of paragraph (1) of this article shall include at least the following issues:

a) The commercial registration information and contact details of the group of undertakings, or group of entities engaged in a joint economic activity.
b) A description of the Personal Data Transfers or set of Transfers, including the categories of Personal Data, the type of processing, its purposes, and the identification of the country or countries to which the data will be transferred.
c) The commitment of all parties to comply with the rules.
d) The application of the data protection provisions, in particular purpose limitation, data minimization, storage periods, legal basis for processing, controls for processing of Personal Data, and the requirements in respect of onward Transfers to bodies not bound by the Binding Common Rules.
e) Rights of Data Subjects regarding Processing and the means to exercise those rights, including the right to file a complaint to the Competent Authority.
f) Provisions for the responsibility of the Controller for any violations of the Binding Common Rules.
g) How the information on the rules is provided to Data Subjects in addition to other information to be provided according to the Law and its Regulations.
h) The tasks of any data protection officer designated or any other person or entity in charge of monitoring compliance with the Binding Common Rules within the group of undertakings, or group of entities engaged in a joint economic activity.
i) The mechanism for processing complaints and dealing with incidents of Personal Data Breach.
j) Mechanisms to ensure and monitor compliance within the group of undertakings, or group of entities engaged in a joint economic activity for ensuring continuous and effective compliance with the Binding Common Rules. Such mechanisms shall

include data protection audits and methods for executing corrective measures. In addition to committing to providing the results of this audit to the Competent Authority upon its request.

k) The mechanism for obtaining approval from the Competent Authority for any amendments to the Binding Common Rules.

l) The cooperation mechanism with the Competent Authority to ensure compliance by each member of the group of undertakings, or group of entities engaged in a joint economic activity.

m) Clarification of regulatory requirements of any Disclosure of Personal Data that the group of undertakings, or group of entities engaged in a joint economic activity in another country is subject to, which may have a negative impact on the provisions and safeguards provided in the rules, and the mechanism for dealing with cases where regulatory requirements outside the Kingdom conflict with the provisions of the Law and its Regulations.

n) The mechanism for training and qualifying personnel having permanent or regular access to Personal Data and Sensitive Data.

3- Adoption of provisions stated in this article shall not limit any of the responsibilities of the Controller as stipulated in the Law and its Regulations.

Article 6: Cases where the appropriate safeguards for Transfer of Personal Data outside the Kingdom are not required

In the absence of an adequate level of protection for Personal Data and in case of inability for the Controller to use any of the appropriate safeguards for data Transfer that are specified in paragraph (1) of Article (5) of this Regulation, the Transfer of Personal Data outside the Kingdom or Disclosure to a party outside the Kingdom is permitted in any of the following cases:

1. The Transfer is necessary for the performance of an agreement to which the Data Subject is a party.
2. If the Controller is a Public Entity and the Transfer or Disclosure is necessary for the protection of the Kingdom's national security or for the public interest.
3. If the Controller is a Public Entity and the Transfer or Disclosure is necessary for the investigation or detection of crimes, or the prosecution of their perpetrators, or for the execution of penal sanctions.
4. Transfer is necessary to protect the Vital Interests of a Data Subject that is unreachable.

Article 7: Cases where Exemptions are not Granted

1. If the Controller transfers Personal Data or discloses it to a party outside the Kingdom in accordance with Article (5) or Article (6) of this Regulation, it shall

immediately stop the Transfer of Personal Data or Disclosure to a party outside the Kingdom in any of the following cases:

a) Transfer or Disclosure affects national security or Vital Interests of the Kingdom.
b) If the results of the risk assessment of personal data transfer outside the Kingdom or disclosing it to a party outside the Kingdom causes high risk to the privacy of Data Subjects.
c) The appropriate safeguards adopted by the Controller are no longer applicable.
d) The Controller is unable to enforce the appropriate safeguards.

2. If any of the conditions stipulated in Paragraph (1) of this Article applies, the controller must do the following:

a) Stop - without undue delay - the process of transferring personal data outside the Kingdom or disclosing it to a party outside the Kingdom.
b) Re-assess the risks of transferring personal data outside the Kingdom or disclosing it to a party outside the Kingdom.

3. The Competent Authority shall continuously evaluate and review the conditions and procedures for revoking the exemption.

Chapter 4: Final Provisions

Article 8: Risk Assessment of Transferring or Disclosing Personal Data outside the Kingdom

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

a) Transfer of data outside the Kingdom in accordance with Article (5) of this Regulation.
b) Transfer of data outside the Kingdom in accordance with Article (6) of this Regulation.
c) Continuous or large-scale Transfer of Sensitive Data outside the Kingdom.

2- The risk assessment of data Transfer outside the Kingdom or Disclosure to a party outside the Kingdom should include at least the following elements:

a) The purpose of the Transfer or Disclosure and its legal basis.
b) Description of the nature of the Transfer or Disclosure to be carried out and its geographic scope.
c) Means and appropriate safeguards adopted for the Transfer of Personal Data outside the Kingdom and the extent to which they are sufficient to achieve the required level of protection for Personal Data.

d) Measures taken to ensure that the Transfer or Disclosure is limited to the minimum amount of Personal Data necessary to achieve the purposes.
e) The material or moral impact that may result from the Transfer or Disclosure, and the possibility of any harm to Data Subjects.
f) Measures to prevent and mitigate identified risks to protect Personal Data.

Article 9: Guidelines

The Competent Authority shall issue guidelines related to the provisions of this Regulation.

Article 10: Enforcement

This Regulation shall come into force from the date of the Law enforcement.


SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority