

Regulation on Personal Data Transfer outside the Geographical Boundaries of 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 pursuant to Royal Decree No. (M/19) dated 9/2/1443 AH and amended pursuant to 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 geographical boundaries of the Kingdom.
- 2- **Transfer of Personal Data:** The Transfer of Personal Data outside the geographical boundaries of 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- The provisions of this Regulation shall not prejudice the provisions of the applicable laws in the Kingdom or the conventions to which the Kingdom is a party.

- 2- The Controller shall comply with the provisions for collecting and processing Personal Data, as well as disclosing it, in accordance with the Law and its implementing Regulations.
- 3- 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 the national security or the Vital Interests of the Kingdom or violate any other law in the Kingdom.
- 4- 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. This shall be determined by using data maps that indicate the need to Transfer or disclose each transferred data and linking it to each processing purpose outside the Kingdom.
- 5- When transferring or disclosing Personal Data outside the Kingdom 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) Data Subject's ability to file a complaint regarding any matter related to their personal data.
 - d) Controller's ability to comply with requirements for notifying Personal Data Breaches.

- e) Controller's ability to comply with provisions, controls, and procedures for disclosing Personal Data.
 - f) Controller's ability to comply with provisions and controls for destroying Personal Data.
 - g) Controller's ability to take necessary organizational, administrative, and technical measures to ensure the security of Personal Data.
- 6- This Regulation shall apply to metadata, operational data, backup data, monitoring systems data, support data, and data derived from Personal Data, in cases where such data directly or indirectly identifies Data Subjects.
- 7- Subject to the provisions of Article 2 of the Law, the provisions of this Regulation shall not apply to the Transfer of Personal Data that does not directly or indirectly identify Data Subjects.

Chapter 2: Transfer based on an Adequate Level of Protection for Personal Data

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

- 1- The Competent Authority shall coordinate with the Ministry of Foreign Affairs, the Ministry of Communications and Information Technology, the Ministry of Investment, the National Cybersecurity Authority, the Presidency of State Security, and the Saudi Central Bank to conduct an assessment of the level of protection for Personal Data outside the Kingdom. The Competent Authority may also coordinate with any other relevant authorities.

- 2- The Competent Authority shall establish rules and procedures for evaluating the level of protection for Personal Data outside the Kingdom.
- 3- The Competent Authority and the authorities mentioned in paragraph (1) of this Article - each according to its jurisdiction - shall evaluate the level of protection for Personal Data outside the Kingdom in accordance with the following criteria:
 - a) The 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) The rule of law, and ensuring the rights of Data Subjects to preserve their privacy.
 - c) The effectiveness of the implementation of the Personal Data protection Laws.
 - d) The 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) The existence of a supervisory authority responsible for monitoring the compliance of controllers with Personal Data protection requirements.
 - f) The willingness of the supervisory authority to cooperate with the Competent Authority of the Kingdom in matters related to Personal Data protection.
 - g) The clarity of regulatory requirements related to the Disclosure of Personal Data by controllers to governmental or regulatory bodies and their non-conflict with the applicable Laws in the Kingdom.
- 4- 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 opinions 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 (3) of Article 3 of the Regulation have been met, as assessed by the participating entities in the assessment of the level of Personal Data protection.

b) Recommending the performance of an international agreement - in accordance with the applicable procedures, according to the circumstances and as estimated by the Competent Authority.

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 (3) of Article 3 of the 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: Exemption

Without prejudice to the provisions of Subparagraph (A) of Paragraph (2) of Article 29 of the Law, a Controller may Transfer Personal Data outside the Kingdom or disclose it to a party outside the Kingdom in the absence of an appropriate level of protection for Personal Data outside the Kingdom compared to the level of protection specified in the Law and the Regulations, in accordance with any of the safeguards specified in Article 6 of the Regulation, or one of the conditions specified in Article 7 of the Regulation.

Article 6: Safeguards for Transferring Personal Data outside the Kingdom

- 1- In the absence of an adequacy decision or international agreement with the country or international organization to which Personal Data will be transferred, the Transfer or Disclosure of Personal Data shall be subject to the condition that the legal requirements in that country or its sectors or the international organization do not

negatively impact the privacy of Data Subjects or their ability to exercise their rights, in addition to adopting any of the following safeguards by the Controller:

- 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 to a standard model issued by the Competent Authority.
- c) Certifications of compliance with the Law and Regulations in the Kingdom, issued by an authorized entity by the Competent Authority.
- d) Binding Codes of Conduct, which are approved by the Competent Authority based on the requests submitted in each case separately.

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

- 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 adopted data protection provisions, in particular purpose limitation, data minimization, storage periods, legal basis for processing, controls for processing

of Personal Data and Sensitive Data, measures to ensure data security, 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 by any party outside the Kingdom.
- 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 the 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 or Regulations.
- n) The mechanism for training and qualifying personnel having permanent or regular access to Personal Data and Sensitive Data.

Article 7: Cases where the Safeguards for Transfer of Personal Data outside the Kingdom are not Applicable

In the absence of an adequacy decision or an international agreement for the Transfer of Personal Data and the inability of the Controller to use any of the data Transfer safeguards specified in paragraph (1) of Article (6) of the 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:

- a) The Transfer is necessary for the performance of an agreement to which the Data Subject is party.
- b) 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.

- c) 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.
- d) Transfer is necessary to protect the Vital Interests of a Data Subject this is unreachable.

Article 8: Cases where Exemptions are not granted

If the Controller Transfers Personal Data or discloses it to a party outside the Kingdom in accordance with Article (6) or Article (7) of the 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) If the Transfer or Disclosure affects national security or Vital Interests of the Kingdom.
- b) If the Transfer or Disclosure causes harm to Data Subjects.

Chapter 4: Final Provisions

Article 9: Risk Assessment of Transferring or Disclosing 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 (6) of the Regulation.

- b) Transfer of data outside the Kingdom in accordance with Article (7) of the 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) The means and safeguards for transferring 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.
- 3- If the results of the risk assessment referred to in paragraph (2) of this article indicate that the Transfer outside the Kingdom or Disclosure to a party outside the Kingdom will harm Data Subjects, national security, or Vital Interests of the Kingdom, the Controller shall take corrective measures and re-conduct the risk assessment.

Article 10: Guidelines

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

Article 11: Revision and Update

The Competent Authority shall review and update the Regulation after three years from the date of issuance, or whenever necessary.

Article 12: Enforcement

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

DRAFT