SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

Risk Assessment Guideline for Transferring Personal Data Outside the Kingdom

Document Classification: Public

February 2025

This document outlines general guidelines for the fundamental steps and detailed phases required to assess the risks associated with transferring or disclosing personal data to entities outside the Kingdom of Saudi Arabia It is intended for reference purposes only and is not legally binding.

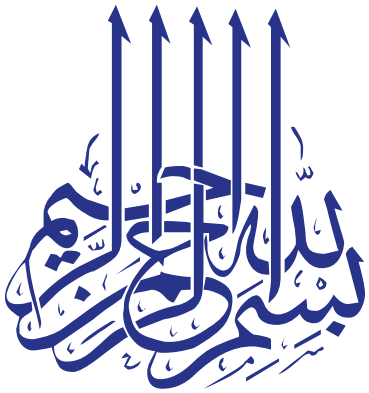
بسم الله الرحمن الرحيم

Table of Contents

Introduction

Given the critical role of issuing guidelines in facilitating the application of the Personal Data Protection Law (the Law), this guideline is designed to assist entities subject to the Law and support the effective implementation of its provisions. The guideline is prepared by the Saudi Data & AI Authority ("Competent Authority") with the aim of explaining the practical steps to assess the risks of transferring or disclosing personal data to entities outside the Kingdom ("Conducting Risk Assessments for Data Transfer and Disclosure). The assessment identifies preparatory steps and concepts, focusing on key measures to evaluate potential risks and negative impacts associated with the processing of personal data.

The terms and phrases contained in this guideline shall have the meanings specified before each of them in the Personal Data Protection Law issued by Royal Decree No. (M/19) dated 9/2/1443H, its amendments, and its Implementing Regulations.

Entities can utilize the supporting tool designed to assess the risks associated with personal data transfer. This tool is available on the platform of the Competent Authority and is intended to assist entities in completing this procedure.

Main Phases of Risk Assessment for Data Transfer or Discloser to Entities Outside the Kingdom

First: Preparation Phase

This phase covers the required steps for conducting a risk assessment for data transfer or disclosure, including evaluating the need to assess potential risks and impacts of processing personal data when offering a service or product to the public. **During this phase, entities should adhere to the following steps:**

A. Determine Whether the Assessment of Potential Risks and Impacts Is Required

This step involves providing a detailed description to determine whether an assessment of the potential risks and impacts of processing personal data is required when offering a product or service to the public. This assessment is based on the presence of any conditions outlined in Paragraph (1) of Article (25) of the Implementing Regulations, **according to the following**:

1. If the processing involves sensitive data.
2. In case of collecting, comparing, or linking two or more sets of personal data obtained from multiple sources.
3. If the controller's activities involve processing personal data on a large scale or on a recurring basis for individuals who have partial or complete legal incapacity. This also applies to processing operations that require continuous monitoring of personal data subjects, the use of emerging

technologies for processing personal data, or automated decision-making based on processing personal data.

4. Offering a product or service that is likely to pose a high risk to the privacy of the data subjects.

B. Description of Product or Service:

This step is designed to provide a detailed description of the service or product involving personal data processing. It helps determine whether the service or product aligns with the entity's activities and defines the purpose for which personal data is collected.

C. Identifying the Purpose:

This step is designed to clearly and accurately define the purpose, ensuring it is identifiable in relation to personal data processing activities in general, and specifically those involving the transfer or disclosure of personal data to entities outside the Kingdom.

D. Identifying the Context of the Personal Data Processing

This step is designed to describe the context of personal data processing, covering all main phases, from collection and retention to use, disclosure, and destruction.

Each phase is described by identifying the personal data processing activities it involves, along with any additional elements relevant to each activity, as appropriate for the phase, as follows:

1. **Collection Phase:** All personal data collection activities should be identified, along with their associated elements, including:

   A. Sources of Personal Data Collection: The sources of personal data collection should be identified, whether obtained directly from the data subjects or through third parties. If the source is a third party, the entity's name must be specified.

   B. Methods of Personal Data Collection All methods of personal data collection, such as electronic forms, cookies, and any other possible methods, should be identified and documented.

2. **Storage/Retention Phase:** All processing activities related to the storage and retention of personal data, including those for operational, archival, or backup purposes, should be identified. The following elements provide a clear description of the activities involved in this phase.

   A. Geographic Location of Storage/Retention: The exact geographical location of personal data storage or retention should be clearly identified, including the specific country where the data is stored.

   B. Place of Storage/Retention: The place where the data is stored or retained should be identified, for example: storage in the public cloud, private cloud, entity’s headquarters, or other storage or retention locations.

   C. Period of Personal Data Retention: The retention period for personal data should be clearly specified, including whether it is based on a

statutory requirement mandating a specific duration or linked to the incomplete fulfillment of the purpose for which the personal data was collected or processed.

3. **Usage Phase:** All personal data processing activities, including remote access for any purpose, should be defined. Each activity must align with the purpose detailed in Paragraph (2) of this section.

4. **Disclosure Phase:** All processing activities related to the disclosure of personal data, along with the entities to which it is disclosed, whether within or outside the Kingdom, should be identified. This includes disclosures to third parties as part of subsequent contracts.

5. **Destruction Phase:** All processing activities related to the destruction of personal data should be defined, whether the destruction is due to the fulfillment of the purpose for which the data was collected or the end of the retention period. This includes specifying the methods used to notify the expiration of the retention period and the secure means employed for destroying personal data.

Second: Assessing Negative Impacts and Potential Risks of Personal Data Processing Phase

This phase involves the steps required to assess the potential negative impacts and risks arising from the processing of personal data when offering a service or product to the public. The process involves the following steps:

1. Linking the elements of negative impact and potential risk assessment, as outlined below, to each activity identified under Paragraph (d) of Clause (I) in this guideline. An international standard for risk assessment and threat analysis may be adopted to define these elements, **taking into account the following:**

   A. Vulnerabilities or Weak Spots: The result of an analysis evaluating the adequacy of measures taken to ensure that each processing activity complies with the provisions, controls, and procedures established by the Law and its Regulations.

   B. Source of Threat: Any source, whether internal or external to the controller or processor, that engages in processing personal data for illegal purposes, whether intentionally or unintentionally.

   C. Expected Event: Any action that exploits existing sources of threats, vulnerabilities, or weak spots, leading to negative impacts on personal data subjects.

   D. Impacts: The level of damage caused by expected events which can be assessed by analyzing the extent of their impact. The impact may affect only the personal data subject, extend to their family and friends, or even reach the broader community.

   E. Probability of Occurrence: The likelihood of an event occurring by evaluating the resources and capabilities available to threat sources that could enable them to exploit weak spots and vulnerabilities.

F. Level of Risk: The result of measuring impact severity relative to the likelihood of occurrence.

2. Analyzing the activities outlined in Paragraph (d) of Clause (I), involving additional elements relevant to each phase. This includes identifying elements associated with assessing the negative impacts and potential risks of processing personal data, as described in this section, and evaluating their levels. These elements include but are not limited to, analyzing the activities related to enabling the personal data subject to access their data held by the controller, which involves evaluating the measures implemented and assessing their adequacy to verify the subject's identity. Insufficient measures in this regard constitute a vulnerability that could be exploited by unauthorized individuals, potentially leading to access or misuse of the data for personal gain or harm to the data subject.
3. Identifying suitable controls and measures to prevent risks, minimize their likelihood, or mitigate their impact when they occur. This is achieved by implementing relevant administrative, technical, and physical controls in accordance with the provisions of Article (19) of the Law and Article (23) of its Implementing Regulation.

Third: Risk Assessment for Data Transfer or Discloser to Entities Outside the Kingdom

This phase includes the steps required to assess the risks of transferring or disclosing personal data to entities outside the Kingdom. During this phase, entities should adhere to the following steps:

1. Risk assessment procedures for the transfer or disclosure of personal data are mandatory:

   The obligation to assess the risks associated with the transfer or disclosure of personal data must be verified by determining the presence of any conditions outlined in Paragraph (1) of Article (VII) of the Regulations, as detailed below:

   a. Transfer of personal data outside the Kingdom or disclosure to entities outside the Kingdom, as specified in Article (IV) of the Regulations.

   b. Transfer sensitive data outside the Kingdom or disclose it to entities outside the Kingdom on a continuous or large scale.

2. If the procedures and steps outlined in Clauses (I) and (II) above are not carried out, they must first be executed, then reviewed, and subsequently

the previous steps in Clauses (I) and (II) should be specified[1], taking into account the following aspects (additional elements related to transfer or disclosure outside the Kingdom):

a. **Nature of Data Transfer or Disclosure:** The nature of data transfer or disclosure involves analyzing phases of transferring or disclosing personal data to entities outside the Kingdom. This includes remote access, collecting personal data for transfer and processing abroad, collecting data of individuals in the Kingdom from external entities, storing or retaining data outside the Kingdom, transferring data for storage or processing outside the Kingdom, and disclosing data to external parties. It also considers the frequency of these operations, their scope regarding categories of data holders, as well as the content of the personal data.

b. **Entities Receiving Transferred Personal Data:** Verifying the compliance of entities receiving disclosed personal data with the

[1]Since the subsequent steps rely on the previous steps outlined in Sections (I) and (II) above, the effectiveness of the guideline depends on ensuring the consistency and integration of these steps to achieve its intended purpose.

provisions of the Law and its Implementing Regulations, particularly those related to disclosure, transit, and subsequent transfer. This includes evaluating the adequacy of the standards and technical measures implemented by the entity to ensure data security, as well as the legal regulations governing the entity/entities to which the personal data will be transferred.

c. Evaluating the adequacy of measures implemented to reduce negative impacts and potential risks, or identifying and applying additional measures to mitigate risk levels.

Fourth: The Guidelines for Identifying Factors Related to the Analysis of Implications for the Vital Interests of the Kingdom

This phase provides guidelines for identifying factors involved in analyzing the impact of transferring or disclosing personal data to entities outside the Kingdom, focusing on the implications for the Kingdom's vital interests as stated in Subparagraph (a) of Paragraph (2) of Article (29) of the Law.[2]

[2] These guidelines may be applied to identify the elements associated with the application of paragraphs (1) and (2) of Article (XVI) of the Law.

After reviewing the impact assessment results for all activities across the specified stages and evaluating the risks associated with transfer or disclosure, **the following considerations shall apply:**

1. The scope of processing, including the content of personal data, the number of data subjects, and their categories.
2. The scope of the impact resulting from the transfer or disclosure of personal data to entities outside the Kingdom (whether limited to the personal data subjects, extending to family and friends, or reaching society at large).
3. The adequacy of technical, organizational, and administrative measures and procedures taken to prevent or mitigate risks.

After completing all steps, reviewing the results, and implementing measures to mitigate, prevent, or reduce risks, the process continues. If the evaluation still indicates high levels of risk and irreversible impacts in the near term on the interests of individuals or the community, the controller should explore alternative methods. This may involve reassessing the necessity of the processing activity in its current form, considering its elimination or modification, or adopting more efficient and effective measures.

SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority