SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

Minimum Personal Data Determination Guideline

Document Classification: **Public**

Version 1.0

August 2024

Notice

The guideline does not replace referring to the Personal Data Protection Law, its Implementing Regulations, and relevant rules and decisions to ensure compliance with the Law's provisions and regulations.

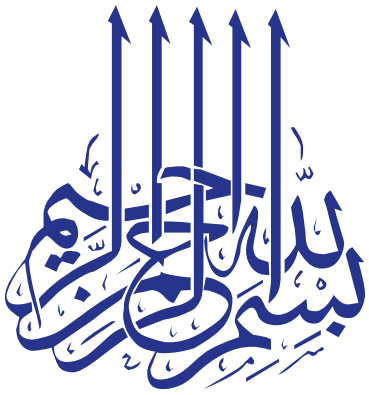
بسم الله الرحمن الرحيم

Table of Contents

Introduction

In recognition of the significance of Data Minimization practices and the importance of achieving the objectives of the Personal Data Protection Law (PDPL) and its Implementing Regulations, this guideline has been developed for entities subject to the PDPL ("the Law") and its Implementing Regulations to assists these entities in fulfilling the purpose of processing Personal Data while avoiding the collection of unnecessary Personal Data. Additionally, it provides practical examples for Controllers to help assess their compliance with Data Minimization controls during processing activities.

Objective

This Guideline aims to:

1. Assist entities in implementing the provisions of the Law.
2. Encourage entities to adopt best practices for Personal Data processing.
3. Provide practical examples for Controllers to assist them in assessing their compliance with the Personal Data processing provisions of the Law and its Implementing Regulations.
4. Protect the privacy of Data Subjects.

First: Minimum Collection of Personal Data

The minimum collection of Personal Data refers to the practice of collecting only the Personal Data that is strictly necessary and directly relevant to the purpose for which it is being collected. This entails avoiding the collection of unnecessary data, adhering to the following principles:

1. **Actual Need:** Each element of Personal Data should be evaluated to determine whether it is directly necessary to achieve the purpose of its collection and processing.
2. **Purpose:** The purpose for which Personal Data is collected must be directly linked to the data itself and directly relevant to the Controller's purposes. It must not conflict with the provisions of other applicable regulations in the Kingdom. The Controller must exercise due diligence in achieving the purpose of processing without collecting unnecessary Personal Data.
3. **Collection Methods:** Personal Data collection methods must be direct, clear, secure, and appropriate to the Data Subject's circumstances. They must also be free from any means that could lead to deception, misleading, or extortion and must not contravene or conflict with the provisions of applicable regulations in the Kingdom.
4. **Content:** The content of Personal Data should be adequate and limited to the minimum necessary to achieve the purpose of its collection, whether it is collected directly from the Data Subject or others. If the Controller achieves the purpose of its collection, the content shall not include anything that could lead to the identification of the Data Subject.
5. **Destruction:** Personal Data that is no longer necessary to achieve the purpose for which it was collected shall be destroyed, following secure procedures to ensure the permanent removal of the data.
6. **Retention:** The Controller shall retain the minimum amount of Personal Data necessary to achieve the purpose of processing, in addition to restricting logical and physical access rights to Personal Data to the minimum privileges and actual need.

Controllers are required to conduct regular assessments to evaluate the Personal Data they retain. This involves the identification and destruction of data that is no longer necessary to fulfill the purposes for which it was collected. Similarly, data that is not relevant to the primary purpose of collection shall also be destroyed. These assessments shall consider the following:

1. Verify that the collected Personal Data is directly relevant or essential for a specific, justifiable purpose.
2. Ensure that the amount of Personal Data collected is limited to what is strictly necessary to achieve the identified and justified purpose.
3. Personal Data shall be retained for a clearly defined period that is necessary to fulfill the purpose of its collection.
4. The Controller must delete Personal Data upon the expiration of the purpose for which it was collected.

Second: What Constitutes “Minimum” Personal Data?

1. While the PDPL does not outline a specific mechanism for determining the "minimum" data necessary to achieve the purpose of processing, Article (11) of the Law stipulates that “the purpose for which Personal Data is collected shall be directly related to the Controller’s purposes, and shall not contravene any legal provisions. Moreover, the content of the Personal Data shall be appropriate and limited to the minimum amount necessary to achieve the purpose of the Collection. Content that may lead to specifically identifying the Data Subject once the purpose of Collection is achieved shall

be avoided. The Regulations shall set out the necessary controls in this regard".

2. The connection between the collection of Personal Data and its predetermined purpose must be clearly and explicitly established. Personal Data shall be collected to the extent necessary to fulfill the collection purpose in accordance with the Data Minimization Principle. No additional data should be collected that is not necessary or directly relevant.

3. Controllers must ensure that their data processing activities are designed to prevent the collection of any unnecessary Personal Data in relation to the specific purposes for which the Personal Data was collected. When designing data processing activities, Controllers must adopt appropriate data management software tools, including those that perform automated periodic reviews to ensure that data remains accurate and up-to-date and that any unnecessary data is destroyed.

Examples:

The following examples serve as guidance for Controllers in assessing their compliance with the Personal Data Minimization Principle:

Example (1)

A recruitment agency distributed details for several open positions that require applicants to provide some data, including health information. It is important to note that this company does not need to collect this type of data except for a limited number of jobs.

In this example, the collection of health information is deemed unnecessary, as

the recruitment agency does not require such data for all job openings. Moreover, collecting Personal Data based on unsubstantiated or uncertain future needs or contingencies must be avoided.

Example (2)

The safety procedures in certain organizations mandate that employers collect the blood types of employees engaged in fieldwork that poses potential risks. This data is crucial for prompt and effective medical intervention in the event of an accident. While it is highly unlikely that this data will be utilized during the employees' tenure, its collection and storage are deemed necessary to minimize the impact of accidents.

In this example, collecting blood type data for employees involved in hazardous fieldwork is deemed necessary and directly linked to the purpose for which it is collected. Therefore, it does not contravene the principle of Data Minimization. However, if blood type data were collected for all employees within the organization, regardless of their role (field, office, or non-risk), such data collection would be deemed inappropriate due to the absence of a compelling necessity.

Third: Controller Obligations:

1. Controllers shall regularly audit and review their Personal Data processing activities to ensure compliance with the Data Minimization Principle. They shall implement appropriate corrective measures through their employees or the Personal Data Protection Officer.
2. When processing Personal Data for a purpose other than that for which it was collected, according to the conditions outlined in Article (10) of the Law, the Controller must ensure that all procedures specifying the data content

are documented, including the operations related to the application of the Data Minimization Principle. The Controller must exercise caution to ensure that the purposes for collecting Personal Data are legitimate and specified. Accordingly, Controllers must not collect Personal Data simply because it is convenient to retain it, as this does not constitute a "necessary" purpose.

3. Controllers must ensure that their employees responsible for collecting Personal Data receive adequate training to understand regulatory obligations regarding Data Minimization. This includes, in particular, training those responsible for designing systems and tools directly involved in the collection and processing of Personal Data to ensure the implementation of the Data Minimization Principle through a "privacy by design" approach.

SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority