SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority

Elaboration and Developing

Privacy Policy Guideline

Document Classification: **Public**

Version 1.0

August 2024

بسم الله الرحمن الرحيم

Table of Contents

Introduction

This guideline aims to guide entities subject to the provisions of Personal Data Protection Law (Law)[1] and its Implementing Regulations, through the preparation and development of their privacy policy, ensuring compliance with the "Right to Be Informed" stated in Article (4) of the Law, and further cited in Article (13) thereof. This also ensures entities' compliance with Article (12) provisions, which obligate entities to prepare a privacy policy, as follows: "The Controller shall use a privacy policy and make it available to Data Subjects for their information prior to collecting their Personal Data. The policy shall specify purpose of Collection, Personal Data to be collected, means used for Collection, Processing, Storage and Destruction, and information about the Data Subject rights and how to exercise such rights".

This guideline shall also provide a standard template that can serve as guidance during the development of entities' privacy policy, to ensure that regulatory requirements are met, and to clarify basic elements that shall be taken into account during policy development. The Law and its Implementing Regulations may be used as reference to determine terms and phrases mentioned in this guideline, and to determine regulatory requirements, as viewing this guideline cannot replace the need to refer to the provisions of the Law and its Implementing Regulations. This guideline is not considered a binding regulatory document, since the Law and its Implementing Regulations provisions serve as regulatory reference for the application of its provisions.

[1] Controllers operating within Kingdom, involved in Personal Data collection and processing, partially or entirely, through any means, as well as Controllers operating outside Kingdom, and involved in collecting and processing Personal Data of individuals residing in Kingdom, through any means, as long as it does not conflict with relevant laws and regulations.

Objective

This guideline aims at:

1. Supporting entities in implementing the Law provisions.
2. Encouraging entities to adopt best practices, ensuring Personal Data privacy and protection.
3. Providing guidance on developing content and design of privacy policy.
4. Helping Data Subjects to exercise their rights stipulated in the Law.
5. Protecting Data Subjects' privacy.

Privacy Policy Key Elements

Privacy policy clarifies Personal Data to be collected, purpose of processing[2], method of use, legal basis for collecting and processing, entities to which such data shall be disclosed, geographical scope of processing, data retention period, method of data destruction, Data Subject’s rights and method of exercising them, and mechanism for communicating with the entity. It also clarifies the entities’ commitment to making individuals’ data available to them in a clear and accessible manner when collected, such as linking it to their websites or applications.

The Controller, depending on the nature of its activity, shall include the legal requirements mentioned below upon preparing its privacy policy:

First: Entity Name and Activity

The Controller shall write its official name in accordance with regulatory registers and trademarks, along with a brief overview of its tasks, specializations, activities, services, and target group.

[2] Articles (5), (6), (10), and (15) of the Law shall be referenced to determine processing legal bases.

Second: Contact Information and Update Record

The Controller shall write its own contact information, including: phone number, website, and postal address. In addition, if the Controller is an entity required to appoint a Personal Data Protection Officer, it shall specify the identity and contact information of the Personal Data Protection Officer to provide further details about the processing of Personal Data and the method of exercising related rights.

Third: Personal Data to Be Collected

The Controller shall clarify Personal Data to be collected either before or during the collection process. Such data can be divided into specific categories as per its type and sources, making it easier for the Data Subject to identify data to be collected clearly and accurately, including, but not limited to:

- Account Data: (Key data collected directly from the user to create an account or personal file, such as name, PIN, addresses, and contact numbers).
- Payment Data: (Data collected for payment purposes, such as bank card number, payment amounts, etc.).
- Data obtained from other parties.
- Cookies Data: (Data collected by website logs, cookies or similar technologies).
- Location Data.

The Controller shall also inform the Data Subject whether collection of this data is mandatory or optional for processing purposes.

Fourth: Collecting Personal Data Methods and Purposes

A. The Controller shall divide methods of collecting Personal Data as specified in Clause (Second) into two main sections of collecting and processing Personal Data:

- **Data to Be Collected Directly from Data Subject:** Clarifying means used for collecting such data, such as e-forms that include empty fields, drop-down lists, radio buttons, etc.
- **Data to Be Collected Indirectly:** Clarifying means used for collecting such data, such as cookies technologies, automatic collection of information, website analytics, or interconnection with another entity.

B. The Controller shall explicitly and clearly clarify the purpose of collecting Personal Data (such as providing public services or a service to Data Subject). Such purposes shall be related directly to the Controller's activity, not contravene with any legal provisions, and specify legal bases relied upon for collecting and processing data, provided that legal basis shall be one of the following: (Consent of Data Subject or his legal guardian; realized interest of Data Subject or legal requirement; agreement to which Data Subject is a party; public interest; security purposes; judicial requirements; protection of public health or safety; or preservation of vital interests of individuals (preserving their health or protecting their lives), or legitimate interests of the Controller).

C. The Controller may rely on more than one legal basis at the same time, in addition to the possibility of collecting or processing Personal Data if it is collected from a publicly available source, in accordance with controls and procedures stipulated in Article (15) of the Implementing Regulation of the Law. Additionally, Personal Data may be processed if it does not include evidence of identity of its owner and the owner's identity has been anonymized as stated in Article (9) of the Implementing Regulation of the Law.

D. In all cases, the content of Personal Data collected and processed shall be limited to the minimum necessary, and directly relevant to the purpose of collection and processing. Data content shall be appropriate, and methods and means of collecting Personal Data shall be clear, direct, and free from deception, manipulation or disinformation.

E. When relying on the Data Subject's consent as a legal basis for processing Personal Data, such consent shall not be a condition for providing a service or a benefit, unless such service or benefit is intimately related and relevant to Personal Data processing.

Fifth: Personal Data Processing

1. The Controller shall clearly and precisely determine the mechanism for processing Personal Data to achieve the purpose stated in Clause (Third) above.
2. To ensure that all uses are comprehensively defined, the Controller may use the main purpose as a general objective and reference basis. Accordingly, a number of specific objectives shall be determined and divided based on the stages of the data life cycle (collecting, storing, using, sharing, and destroying). At each stage, a specific objective is divided into a group of general data processing operations, and for each general operation, a specific operation shall be determined that is carried out on a specific set of data.
3. The Controller may present the method of using and displaying data in a table format or in a clear text that clarifies each statement and method of usage.

Sixth: Personal Data Sharing

1. The Controller shall clarify whether Personal Data or a specific group thereof shall be disclosed to other entities (whether inside or outside the Kingdom) and shall provide the Data Subject with information about the entity(s) to which Personal Data is disclosed, along with a description of such entities.
2. If there is a need to disclose Personal Data or a specific group thereof, the main purpose of disclosing such data shall be clearly and accurately specified, along with whether it will be disclosed occasionally (one time) or regularly (several times).

Seventh: Personal Data Storage, Retention Period, and Destruction

1. The Controller shall clarify the means used to store Personal Data and its geographical locations, whether stored on servers at the Controller's headquarters or on servers of an external entity, such as cloud computing service providers (whether inside or outside the Kingdom).

2. The Controller shall clarify the time period to retain Personal Data and shall specify the retention period for each type of Personal Data in accordance with regulatory requirements. The Controller shall also clarify methods used to destroy Personal Data after its intended purpose is fulfilled, ensuring that it cannot be viewed or recovered.
3. The Controller shall clarify necessary administrative, technical, and organizational means and measures that have been taken to protect Personal Data from incidents of leakage, damage, or illegal access, including, but not limited to, the use of data encryption, anonymization, and coding methods. The Level of security measures shall also depend on the sensitivity and amount of Personal Data collected.

Eighth: Personal Data Subjects Rights

The Controller shall clarify the rights of Data Subjects regarding the collection and processing of their data as specified in Law, along with the method of exercising these rights. The Controller shall also provide appropriate communication channels to respond to Data Subjects' requests related to their rights according to their choice and availability. These channels may include: (emails, text messages, communication via electronic applications). The Controller shall also specify the time taken for response.

1. The Right to be informed, which includes informing Data Subjects of the legal basis and purpose of collecting data while ensuring that Data Subjects' data will not be subsequently processed in any way inconsistent with the purpose of collecting such data, for which Data Subjects provided their explicit or implicit consent.
2. The Right to access their Personal Data held by the Controller, which includes Data Subjects' access to their Personal Data upon request or through means provided by the Controller that enables Data Subjects to have access to their Personal Data Automatically without the need to submit a request.
3. The Right to request access to Personal Data held by the Controller in a readable and clear format consistent with the content of records, whether such Personal Data is in a commonly used format if feasible, or providing a printed hard copy of such data.
4. The Right to request correction, completeness, and update of Personal Data held by the Controller.
5. The Right to request the destruction of Personal Data held by the Controller if Personal Data is no longer necessary to achieve the purpose for which it was collected.

6. The Right to withdraw consent for Personal Data Processing at any time, unless there is a legal basis that requires otherwise, in addition to elaborating how to withdraw such consent by providing means and methods to ensure a prompt response to requests related to exercising rights according to measures stated in Article (12) of the Implementing Regulation of the Law.
7. The Right to submit any complaint related to applying the provisions of the Law to the Competent Authority.
8. The Right to claim compensation for material or moral damage if the Data Subject is harmed as a result of any violation stipulated in the Law and its Implementing Regulations.

Ninth: Complaint and Objection Filing Mechanism

The Controller shall provide a mechanism for filing complaints and objections if there is a complaint by Data Subjects, such as failure to enable them to exercise their rights related to the processing of Personal Data within the period specified in the Clause (Eighth) above, or if there are objections to processing. This can be made by determining the name of the department or division involved in receiving and processing complaints, its contact details, and the period specified for processing such complaints, in addition to providing information about the Competent Authority[3] in the event of Data Subjects' dissatisfaction with the results of complaint processing by the Controller.

[3] Saudi Data & AI Authority.

Tenth: Availing and Providing Access to Privacy Policy

The Controller shall provide access to the Privacy Policy and ensure that its content is written in clear, non-misleading, easy-to-read, and understandable language suitable for the comprehension level of all categories of Data Subjects. In addition, the necessary measures shall be taken to notify individuals of the Privacy Policy, as privacy notification is one of the primary ways to inform individuals about the collection of their data. This can be done through app notifications, SMS, e-mails, or a standalone form provided to Data Subjects before or during the collection and processing of their Personal Data.

The Controller shall periodically review the Privacy Policy and record any amendment or update introduced thereto in the update record stated in the Clause (Second) hereinabove.

In addition, any of the following methods can be followed:

- Adding pictures and icons that express the content of clauses and paragraphs in a manner that facilitates the reader's quick understanding of the content.
- Reordering and titling clauses and paragraphs in a logical manner that stimulates rapid reading and comprehensing.
- The Privacy Policy shall be designed in a clear and understandable manner for specific groups if the entity aims, in full or in part, to process data of such special segments (children, elderly, persons with disabilities).
- The Privacy Policy shall be designed in a language suitable for the target audience.
- Adding other related links to the Privacy Policy, such as Terms & Conditions, Cookie Policy, and Personal Data Protection Law.

Detailed Model for Privacy Policy

[Entity Name]

[An overview of the entity's responsibilities and functions, services provided and target audience]. You can contact us via various available channels, using the below contact details.

Contact Details

Involved Department/Team:

[ ]

Address:

[ ]

Phone Number:

[ ]

E-mail:

[ ]

License or Commercial Register:

[ ]

Date of Last Update

The Privacy Policy was last updated on [date of last update]. You can review the update history through [You can add a link or attach the update table if the Policy is a hard copy].

What Personal Data is collected?

We collect and process the following Personal Data:

- [Add data that is collected, which can be categorized, for example, into master data and contact details]

How do we collect your Personal Data? What is the purpose for collection?

Some of the Personal Data that we process is obtained **directly from you** using [Specify collection method] for the following purposes:

- [Add the purposes for which Personal Data is collected, which can be categorized by types of data.]

We also obtain some Personal Data **indirectly** from the following sources:

- [Add sources through which Personal Data is collected indirectly, including the collection method, while stating the purpose of collection. Sources can be categorized by types of data and their sources.]

How do we use your Personal Data?

We use Personal Data collected, directly or indirectly, as follows:

- [Add how you use Personal Data]

How do we disclose your Personal Data?

[We will not disclose your Personal Data to any third party for direct marketing purposes.] Or [we may disclose your Personal Data to the following entities:]

- [Add entities to which the Personal Data will be disclosed while stating the purpose for each type of data.]

Legal Basis for Collecting and Processing Your Personal Data

In accordance with the Personal Data Protection Law, the legal basis on which we rely in processing such data is: (One legal basis or more can be selected from the below bases)

- Your explicit consent. You can withdraw your consent at any time without affecting processing operations carried out based on other legal bases. To this end, you can contact [Name of the involved department/division or Personal Data

Protection Officer].

- In fulfillment of a contractual obligation [Such obligation and the importance of fulfilling it shall be stated].
- In compliance with a statutory obligation [Name of the law and article that authorizes the entity to collect and process Personal Data shall be stated].
- Maintaining vital interests [Method of maintaining vital interests by collecting and processing Personal Data shall be stated].
- Achieving public interest [The public interests to be achieved by collecting and processing Personal Data shall be stated].
- Achieving legitimate interests or objectives [The legitimate objective that does not conflict with Data Subject rights shall be stated]

How do we store your Personal Data?

Your Personal Data is stored securely either at the headquarters/or at a cloud computing service provider [Add location where Personal Data is stored or hosted]. We also retain [Specify the type of Personal Data] for a period of [Number of months], after which we will securely dispose of such data in a manner that prevents access or retrieval, using [Describe the method of data destruction]. (Retention period for each data type shall be determined separately).

Your Rights Regarding Processing of Your Personal Data

Under Personal Data Protection Law, you have the following rights, which primarily depend on the purpose of Personal Data collection and processing:

- **Right to Be Informed:** You are entitled to be informed how we collect your personal data, legal basis for collection and processing, how such data is processed, stored, destroyed, and to whom it will be disclosed. You can access all details through the Privacy Policy or contact us using the below mentioned information. (Elaborate on any restrictions to the right to be informed in a simple language).

- **Right of Access to Your Personal Data:** You are entitled to request access to your Personal Data through [Means through which you have access to Personal Data]. (Elaborate on any restrictions to the right to access in a simple language).
- **Right to Request Access to Your Personal Data:** You are entitled to request access to your Personal Data held by the Controller in a readable and clear format if technically feasible through [Means through which Data Subjects are provided with their data]. (Elaborate on any restrictions to the right to access in a simple language, including restrictions and exemptions, if any).
- **Right to Request Correction of Your Personal Data:** You are entitled to request correction of your Personal Data that you believe is inaccurate, incorrect or incomplete, through [Means through which correction can be requested]. Such data will be reviewed and updated within [Number of days]. In addition, you will be notified through [Means through which Data Subjects can have access to their data].
- **Right to Request Destruction of Your Personal Data:** You are entitled to request destruction of your Personal Data in certain circumstances (Possible cases shall be elaborated in a manner that does not contradict legal bases and the right to destruction).
- **Right to Withdraw Your Consent for Processing Your Personal Data:** You are entitled to withdraw your consent for processing your Personal Data at any time unless there are legal bases that require otherwise.

Unless otherwise stipulated by the law, you will not be required to pay any fees in return for exercising this right. In case of submitting a request for exercising this right, you will receive a response within [Number of days] as of the request receiving date.

For further details regarding the processing of your Personal Data and how to exercise your rights, you can contact the Personal Data Protection Officer at the [Entity] using the below mentioned contact details.

Personal Data Protection Officer

Name:

[ ]

Address:

[ ]

Phone Number:

[ ]

E-mail:

[ ]

Complaint or Objection Filing Method

If you have any concerns, or if we do not comply with the Personal Data Protection Law, you can file a complaint to [Add name of department or division responsible for handling complaints] using one of the following channels: [Add method and contact details of receiving complaints and inquiries].

If you are not satisfied with how we process your complaint, or if we fail to respond within [Number of days], you can file a complaint to the Competent Authority [Add SDAIA name].

SDAIA Address

Kingdom of Saudi Arabia

Riyadh

Website

Saudi Data & AI Authority (sdaia.gov.sa)

National Data Governance Platform "DGP" (dgp.sdaia.gov.sa)

SDAIA

الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority