SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

Rules for Appointing Personal Data Protection Officer

Document Classification: **Public**

Version 1.0

August 2024


بسم الله الرحمن الرحيم

Table of Contents

Introduction

Saudi Data & AI Authority "SDAIA" issued these Rules based on Paragraph (2) of Article (30) of Personal Data Protection Law issued pursuant to Royal Decree No. (M/19) dated 09/02/1443 AH and amended pursuant to Royal Decree No. (M/148) dated 05/09/1444 AH, and Paragraph (4) of Article (32) of the Implementing Regulations of the Law.

Article 1: Definitions

1- The terms and phrases mentioned herein shall have the meanings ascribed thereto in Article (1) of Personal Data Protection Law, hereinafter referred to as the "Law", issued pursuant to Royal Decree No. (M/19) dated 09/02/1443 AH and amended pursuant to Royal Decree No. (M/148) dated 05/09/1444 AH and Article (1) of the Implementing Regulations of the Law, unless they have a specific definition herein.

2- The following terms and phrases, wherever mentioned herein, shall have the meanings ascribed thereto, unless the context requires otherwise:

3- **Competent Authority:** Saudi Data & AI Authority (SDAIA).

4- **Data Protection Officer (DPO):** One or more natural persons appointed by Controller to be responsible for monitoring the implementation of the provisions of the Law and its Implementing Regulations, overseeing procedures applicable by Controller, and receiving requests relate to Personal Data in accordance with provisions of the Law and its Implementing Regulations.

5- **Core activities:** Activities conducted by the Controller to achieve its core objectives.

Article 2: Purpose

These Rules aim at:

1- Setting minimum requirements for appointing DPO.

2- Clarification of concepts related to cases in which Controller shall appoint DPO.

3- Determining DPO Roles & Tasks

Article 3: Scope of Application

These Rules shall apply to all Controllers covered by provisions of the Law and its Implementing Regulations.

Article 4: Requirements for DPO Appointment

1- When appointing DPO, Controller shall ensure that the following requirements are met:

   A. Having appropriate academic qualifications and experience in the field of Personal Data protection.

   B. Sufficient knowledge of risk management practices, including the management and handling of personal data breach incidents.

   C. Having sufficient knowledge of regulatory requirements for Personal Data protection and other relevant regulatory requirements for performing DPO tasks.

   D. Honesty and integrity, and not having been convicted of any offense involving dishonesty or breach of trust.

2- DPO may be an executive, employee of Controller or an external contractor.

Article 5: Cases of Appointing DPO

First: Controller shall appoint one or more individuals to be responsible for protection of Personal Data in any of the following cases:

1- Controller is a Public Entity that provides services involving Processing of Personal Data on a large scale.
2- Controller core activities are based on processing operations that, by their nature, require regular and systematic monitoring of Data Subjects.
3- Core activities of Controller are based on processing of sensitive Personal Data.

Second: The determination of whether the processing is on a large scale is based on the following criteria:

1- Number of data subjects.
2- Volume of personal data.
3- Type of personal data.
4- Geographical scope of processing.
5- Different categories of data subjects.

Third: The term “regular and systematic monitoring of Data Subjects” refers to:

1- Collection of personal data through tracking or other technologies.
2- Monitoring is considered regular if it is continuous, occurs at specific intervals, or takes place periodically.
3- Monitoring is considered systematic if it is conducted through technological systems, follows a specific methodology, or is implemented

as part of a comprehensive strategy or general plan for collecting personal data.

Fourth: The following activities are examples of regular and systematic monitoring:

1- Collecting personal health and fitness data through wearable devices.
2- Using behavioral analytics technologies for risk assessment purposes.
3- Location tracking, the use of cookies, and surveillance cameras.

Fifth: Activities are considered core if the Controller cannot provide products or services without processing personal data. Examples of core activities include:

1- Insurance companies processing health data to provide health insurance to customers.
2- Finance companies processing credit data to offer products or services related to financing.
3- Marketing companies processing personal data for marketing purposes.

Activities that support the Controller's core business, such as processing employee data by the human resources department within the entity, do not constitute core activities.

Article 6: Documenting DPO Appointment

1- The DPO must be appointed in writing, and the Controller must:
   A. Document the appointment of the DPO if they are an employee of the Controller.
   B. Conclude an agreement with the external contractor when appointing a contractor outside the Controller as the DPO.

2- The appointment of the DPO and their contact details must be promptly announced within the Controller.

Article 7: DPO Contact Details

1- The Controller must provide a clear and accessible means of communication with the DPO for data subjects.

2- The Controller must provide the competent authority with the DPO's contact details immediately upon their appointment, through the National Data Governance Platform, and update these details when the DPO changes.

Article 8: DPO Roles & Tasks

DPO shall be responsible for performing tasks stated in Paragraph (3) of Article (32) of the Implementing Regulation of the Law, in addition to the following tasks:

1- Providing support and advice regarding all aspects of Personal Data protection, including contributing to developing policies and internal procedures related to Personal Data protection at Controller.

2- Participating in awareness activities, training and transfer of knowledge to Controller personnel regarding Personal Data protection and compliance with provisions of the Law, Implementing Regulations and ethics of data handling.

3- Contributing to reviewing plans of response to Personal Data Breach incidents, and ensuring that such plans are adequate and effective.

4- Preparing periodic reports regarding Controller activities related to processing of Personal Data, and providing recommendations to ensure compliance with provisions of the Law and its Implementing Regulations.

5- Following up on regulatory documents issued by the competent authority related to the protection of personal data, including any amendments, and inform the relevant departments to ensure compliance.
6- Providing support and advice to those responsible for developing and operating modern technological systems to ensure compliance with the requirements of the Law and its Implementing Regulations.

Article 9: General Provisions

1- Controllers shall periodically review DPO appointment cases to determine whether such cases are still required or likely to become mandatory according to provisions hereof.
2- The Controller may appoint a DPO on a voluntary basis, even if not obligated to do so, to assist in complying with the provisions of the Law and its Implementing Regulations.
3- When concluding an agreement between the Controller and the Processor for processing personal data on behalf of the Controller, the Controller shall verify whether the Processor has a DPO. If the appointment of a DPO is required under these rules, the Controller should request the appointment to ensure that the necessary guarantees for implementing the provisions of the Law and Implementing Regulations are in place.
4- The Controller must enable and support the DPO in performing their duties and responsibilities by providing all necessary resources.
5- When appointing DPO, Controller shall not assign tasks that may conflict with DPO tasks or affect DPO's independence.

6- The Controller shall work on training and developing DPO's in the fields of Personal Data protection and support them in obtaining professional certificates in this field to ensure raising their efficiency.

7- The DPO shall be organizationally linked to the Data Management Office within the Controller. If the Controller is not obligated to establish a Data Management Office, the DPO should be linked to another department, in accordance with paragraphs (4) and (5) of this article.

Article 10: Review and Amendment

The Competent Authority shall review these Rules when required, and may introduce any amendment or update thereto.

Article 11: Entry Into Force

These Rules shall come into force as of the date of publishing on the Competent Authority's official website.

SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority