SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

Personal Data Breach Incidents Procedural Guide

Document Classification: Public

Issue No. 1.0

October 2024

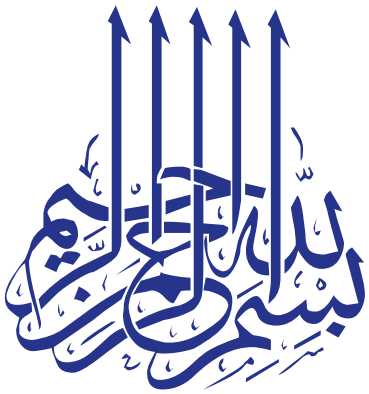
بسم الله الرحمن الرحيم

Table of Contents

Introduction

Within the framework of the Saudi Data & AI Authority (SDAIA) in supporting the Controller in adhering to the provisions of the Personal Data Protection Law issued by Royal Decree No. (M/19) dated 09/02/1443 AH, amended by Royal Decree No. (M/148) dated 05/09/1444 AH, and its Implementing Regulations, which state that if the Controller knows about any personal data breaches, it shall notify SDAIA in accordance with the conditions set forth in the Regulations, along with notifying the Data Subjects if this incident harms their data or conflicts with their rights or interests. SDAIA prepared this Guide in order to outline the necessary procedures to deal with personal data breaches and reduce the consequences and risks influencing Data Subjects in accordance with the Law and its Implementing Regulations.

Definitions

The following words and expressions shall have the meanings mentioned thereto in the definitions included in the Personal Data Protection Law issued by Royal Decree No. (M/19) dated 09/02/1443 AH, and amended by Royal Decree No. (M/148) dated 5/9/1444 AH and implementing regulations thereof. The following words and expressions shall have the meanings mentioned thereto unless the context requires otherwise:

#	Term	Definition
1	Guide	Procedural Guide for Handling Personal Data Breach Incidents.
2	SDAIA	Saudi Data & AI Authority
3	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.

Scope

This Guide applies to all controllers subject to the provisions of Personal Data Protection Law and Implementing Regulations.

Stages of the Personal Data Breach Incidents Response

STAGE ONE: SDAIA Notice

Without prejudice to submitting any report or notice of personal data breach pursuant to Regulations issued by the National Cybersecurity Authority (NCA) and any applicable regulations and rules in the Kingdom of Saudi Arabia, the Controller shall notify SDAIA within a period not exceeding (72) hours from the time it becomes aware of the incident and if the incident is expected to harm the personal data or data subjects or is in conflict with their rights or interests through personal data breach notification service provided by National Data Governance Platform**.** Registration on this platform is required to utilize such service. Upon a personal data breach, the Controller is required to compile a notice that includes:

1. Description of the personal data breach, including the time, date, how it occurred, and when the Controller became aware of the incident.
2. Category of Data Subjects, their actual or approximate numbers, type and nature of the personal data.
3. A description of risks arising from personal data breach, detailing actual or potential consequences and risks to personal data or the Data Subject, the remedial actions undertaken by Controller to prevent, mitigate, or minimize those risks. Furthermore, identifying appropriate future measures the Controller will implement to prevent or avoid the recurrence of the incident.
4. Indicating whether Data Subject has been or will be notified of personal data breach, breach in accordance with the requirements mentioned in the second stage of this guide.

5. Contact details of the Controller or its personal data protection officer (if any) or any other person who has information about the incident being reported.

NOTE: Upon subsequent contracts as stated in Article (8) of the PDPL, the Processor or any other entity shall follow the above Notice Requirements in coordination with the Controller.

STAGE TWO: Breach Incident Containment

The Controller shall implement response and containment procedures for personal data breach incident in accordance with best international practices and relevant regulatory requirements, including, but not limited to, the following measures to control personal data breach incidents:

1. Identifying type and quantity of personal data.
2. Identifying type of breached personal data that can be changed (such as email addresses, passwords, confidential inquiries, credit card numbers, etc.) and taking actions to change this breached data.
3. Identifying individuals affected by data breach incident based on type of personal data breached.
4. The Controller shall notify the Data Subjects without undue delay if this results in damage to their data or conflicts with their rights or interests, including, but not limited to: Damages related to exercising the right of the data subject, physical harm such as stalking and assault, or economic damage, such as fraud or identity theft.

   A. Notice Methods:

   1. The Controller may notify the Data Subject by any appropriate means in accordance with the preferred methods for communication by the Data Subject, including, but not limited to text messages, or e-mail.
   2. If the breach damage extends to a large group of people at the national level, the Controller may, provided, that the content of the notice complies with the applicable law requirements in the Kingdom, in addition to the provisions mentioned in paragraph (1) above, notify the Data Subject by

other means, including, but not limited to, Controller's website, official controller's accounts on social media platforms, or media.

B. Notice Description:

The notice provided to the Data Subject shall be in a clear and simple manner and shall include the following:

1. A detailed explanation of personal data breach incident.
2. An explanation of the potential risks arising from that incident and the measures taken to prevent, avoid, or mitigate such consequences.
3. The Controller's Name, contact details and its DPO (if any) or any other appropriate means of communication with the Controller.
4. Guidelines and necessary advice that may assist the affected Data Subject in taking appropriate actions to avoid potential risks or mitigate their consequences, such as economic damages ex. fraud or identity theft.

STAGE THREE: Documentation

The Controller shall retain copies of the documents submitted to SDAIA regarding incidents of personal data breach, the corrective actions taken, and any relevant proper records or documents. The Controller shall take all corrective actions to contain personal data breach incidents, in accordance with lessons learned from it.

SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority