SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

Personal Data Destruction, Anonymization, and Pseudonymisation Guideline

Document Classification: **Public**

Version 1.0

August 2024

Notice

This 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.

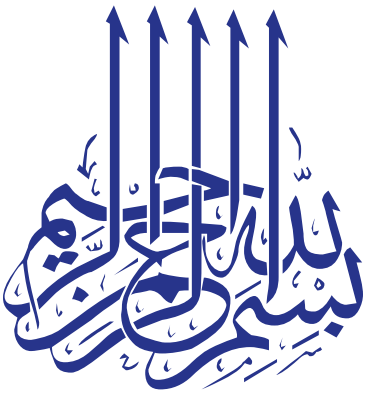
بسم الله الرحمن الرحيم

Table of Contents

Introduction

In fulfillment of its mandate to raise awareness among entities subject to the provisions of the Personal Data Protection Law the "Law" and its Implementing Regulations, and to enable those entities to understand their obligations under Article (18) of the Law and Articles (8) and (9) of the Implementing Regulations, the Saudi Data & AI Authority (SDAIA) has issued this Guideline to assist entities in determining the cases where personal data should be destroyed or anonymized. This Guideline also provides examples of techniques to aid in the destruction ,anonymization and Pseudonymisation of personal data. The terms and phrases used in this Guideline shall be construed in accordance with the definitions provided in the Law and its Implementing Regulations. This Guideline shall not be considered a binding legal document, nor shall it substitute consulting the Law and its Implementing Regulations, which shall constitute the regulatory reference for all matters related to the application of the Law's provisions.

Objectives

This Guideline aims to:

1- Assist entities in implementing the provisions of the Law.
2- Encourage entities to adopt best practices for personal data destruction, anonymization, and Pseudonymisation.
3- Provide technical examples to aid Controllers in implementing the provisions concerning data destruction, anonymization, and Pseudonymisation as outlined in the Law and its Implementing Regulations.
4- Contribute to empowering data subjects to exercise their rights as stipulated in the Law.

5- Protect the privacy of data subjects.

First: Personal Data Destruction

In cases where the Controller is required to destroy personal data, it shall ensure that the data is permanently and irrevocably deleted, rendering it inaccessible, unrecoverable, and unidentifiable. Data archiving or backup processes shall not be considered data destruction techniques. Such processes shall be treated as personal data in accordance with the Law and its Implementing Regulations. Additionally, the Controller shall comply with the requirements of Article 18 of the Law and other applicable data destruction regulations. This Guideline does not relieve entities of their obligation to adhere to relevant controls, standards, and rules issued by the National Cybersecurity Authority or other competent authorities.

1- **Destruction Circumstances: The Controller shall destroy personal data in any of the following casas:**

A) Upon the request of the data subject.

B) If the personal data is no longer necessary to fulfill the purposes of its collection.

C) If the data subject withdraws their consent to the collection of their personal data, where consent was the sole legal basis for data processing.

D) If the Controller becomes aware that the personal data is being processed in a manner that violates the Law.

2- **Destruction Conditions: The Controller, upon the destruction of personal data, shall:**

A) Take appropriate measures to notify other entities to whom the Controller has disclosed the relevant personal data and request that they destroy it.

B) Take appropriate measures to notify individuals to whom personal data has been disclosed by any means and request that they destroy it.

C) Destroy all copies of the personal data stored in the Controller's systems, including backups, taking into account any relevant regulatory requirements.

3- Examples of Destruction Techniques:

A) **Data Overwriting and Secure Erasure (SE):** Data overwriting involves replacing original data with random, meaningless data, rendering the original data irretrievable. Secure erasure is a more advanced data deletion technique than overwriting. It involves issuing a command to the device's software to delete all data, including data residing in sectors not typically accessible through standard deletion processes.

B) **Data Erasure (without Physical Media Destruction):** This technique involves utilizing a degaussing device to neutralize the magnetic field that stores data, thereby rendering the data effectively unreadable. Degaussing is a secure and efficient technique that preserves the physical integrity of the storage device for reuse, making it the preferred technique for bulk data erasure operations. However, degaussing is limited to magnetic media and is not applicable to solid-state drives (SSDs) or flash-based storage.

C) **Shredding and Distortion:** Shredding assets into tiny shreds and physically distorting them to render the assets effectively unreadable.

Second: Anonymization

The Controller shall ensure that all direct and indirect personally identifiable information is irreversibly anonymized, rendering the data subject unidentifiable. Data that has been rendered anonymous shall no longer be considered personal

data and, consequently, shall not fall within the scope of the Personal Data Protection Law.

The Controller, upon the anonymization of personal data, shall:

A) Ensure that the anonymized data is rendered irreversibly anonymous, making it impossible to re-identify the data subject.

B) Conduct an impact assessment, including an evaluation of the potential for re-identification under the circumstances specified in Paragraph (1) of Article 25 of the Implementing Regulation.

C) Implement appropriate organizational, administrative, and technical measures to mitigate risks, ensuring that these measures are up-to-date and aligned with technological advancements and evolving anonymization techniques.

D) Evaluate the effectiveness of implemented anonymization techniques and implement requisite adjustments to ensure the sustained irreversibility of the anonymization process.

Third: Pseudonymisation

Pseudonymisation is defined as the process of transforming primary identifiers that reveal the identity of the data subject into codes that render the direct identification of the data subject infeasible without the use of additional data or information. Such additional data or information shall be maintained separately and subjected to adequate technical and administrative controls to ensure that it cannot be definitively linked to the data subject.

Pseudonymised data is considered personal data because it may be used, in one way or another, to identify a specific individual. “Pseudonymisation” serves as a protective measure for personal data and is deemed an appropriate technical safeguard against the risks associated with personal data processing. However,

its effectiveness in safeguarding personal data is not equivalent to that of “anonymization”. One example of Pseudonymisation is substituting one or more of the data subject's PII elements. For instance, the name is substituted with a symbol (such as a reference number).

Pseudonymisation shall be applied whenever personal data, including personal data linked to an individual other than the data subject, is disclosed. In such instances, the personal data of the individual shall be Pseudonymised to ensure their privacy. Pseudonymisation shall also be applied when personal data is collected or processed for scientific, research, or statistical purposes without the data subject's consent, provided that such Pseudonymisation does not compromise the purpose for which the data is being processed.

Examples of Anonymization and Pseudonymisation Techniques:

Technical measures employed to anonymize and Pseudonyms personal data vary depending on the specific data being processed and the Controller's regulations. These measures must be regularly reviewed and updated to ensure that the data cannot be linked to a specific data subject.

Examples of Commonly Used Techniques:

A) Data Generalization: The substitution of specific attributes with more generalized values. For instance, aggregating ages into age bands (20-30, 30-40) rather than using precise age values.

B) Data Aggregation: The consolidation of individual data points into a range, group, or category, for instance, recording only the birth year instead of the full birthdate. It should ensured that the aggregated data cannot be used to infer information about specific individuals.

C) Data Encryption: The process of transforming personal data into a secure code using robust cryptographic algorithms. Cryptographic keys must be stored securely and separately from the encrypted data.

D) Data Masking: The application of data masking techniques to conceal or obscure specific data elements.

Fourth: General Guidelines

1- All activities involving data anonymization, destruction, and Pseudonymisation shall be conducted in compliance with the Personal Data Protection Law, its Implementing Regulations, and any applicable regulatory requirements issued by relevant competent authorities.

2- All employees involved in data security shall be adequately trained on the importance of secure data Pseudonymisation and anonymization.

3- The Controller shall ensure that no personal data is lost, misplaced, or disclosed to any unauthorized third party during the destruction, anonymization, or Pseudonymisation process.

4- All printed documents shall be disposed of in a manner that renders the personal data irretrievable (e.g., shredding using secure shredding machines and disposing of the waste securely) in accordance with the regulatory requirements issued by relevant competent authorities.

5- Detailed records shall be maintained of all data anonymization and destruction activities, including the techniques used, the justification for their selection, and ensuring that such records are available upon request from the competent authority.

6- The Controller shall regularly review and update its data anonymization, destruction, and Pseudonymisation techniques to address emerging risks and technological advancements.


SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority