Data Subject Rights Management Processes

Saudi Commission for Health Specialties (SCFHS)

Date: 02/12/2024

1. Objective

To define a structured and compliant process for managing the rights of Data Subjects as outlined by SDAIA NDMO, PDPL, and applicable regulations. This process ensures that Data Subjects can exercise their rights effectively while safeguarding their personal data.

2. Scope

This process applies to all Data Subjects whose personal data is processed, stored, or transmitted by the SCFHS, including employees, customers, vendors, and third parties. It addresses requests related to access, rectification, erasure, restriction, portability, and objection.

3. Definitions & Overview

1. **Data Subject**

   An individual whose personal data is processed by the SCFHS.

2. **Data Protection Officer (DPO)**

   The designated individual responsible for overseeing compliance with data protection laws and handling Data Subject requests.

3. **Personal Data**

   Any information related to an identified or identifiable individual.

4. **Supervisory Authority**

   SDAIA NDMO or any other authority designated under PDPL for overseeing personal data protection.

Data subjects are entitled to exercise the following rights under data protection laws:

1. **Right to Access**

   Request a copy of personal data held by the SCFHS.

2. **Right to Rectification**

   Correct inaccurate or incomplete personal data.

3. **Right to Erasure (Right to Be Forgotten)**

   Request deletion of personal data under certain conditions.

4. **Right to Restriction**

   Restrict the processing of personal data under specific circumstances.

5. **Right to Data Portability**

   Receive personal data in a commonly used, machine-readable format.

6. **Right to Object**

   Object to processing based on legitimate interests or direct marketing.

7. **Right to Withdraw Consent**

   Withdraw previously given consent for data processing.

8. **Right to Not Be Subject to Automated Decision-Making**

   Challenge decisions made solely through automated processing.

4. Process Steps

Step 1: Receiving and Acknowledging Data Subject Requests

1. **Request Submission Channels**

   a. Provide multiple channels for submitting requests, such as:

      i. Online forms on the SCFHS's website.
      ii. Dedicated email addresses for privacy-related inquiries.
      iii. Physical submission at designated locations.

2. **Acknowledgment of Requests**

   a. Acknowledge receipt of the request within **2 business days**.

b. Include the following in the acknowledgment:

i. Reference number for tracking.
ii. Expected timeline for response.
iii. Contact details for further queries.

3. **Verification of Identity**

a. Verify the identity of the Data Subject before processing the request:

i. Request government-issued identification or other valid documentation.
ii. Ensure the verification process complies with data minimization principles.

Step 2: Classifying and Validating Requests

1. **Types of Data Subject Requests**

a. Access

Request for copies of personal data processed by the SCFHS.

b. Rectification

Correction of inaccurate or incomplete data.

c. Erasure

Deletion of personal data (right to be forgotten).

d. Restriction

Limiting processing of personal data under specific conditions.

e. Portability

Transfer of personal data to the Data Subject or a third party.

f. Objection

Objecting to processing based on legitimate interests or direct marketing.

2. **Validation of Requests**

    a. Ensure requests meet regulatory requirements:

        i. Access requests must specify the data or timeframe involved.
        ii. Erasure requests must comply with retention policies and legal obligations.
        iii. Portability requests must involve data provided by the Data Subject.

3. **Rejecting Invalid Requests**

    a. Inform the Data Subject if the request is invalid, providing clear reasons and guidance on submitting valid requests.

Step 3: Processing Data Subject Requests

1. **Internal Coordination**

    a. Forward the request to relevant departments (e.g., IT, Legal, HR) for processing.
    b. Maintain strict confidentiality throughout the process.

2. **Timeline for Response**

    a. Respond to all valid requests within **30 days**, extendable by 30 additional days for complex cases.
    b. Notify the Data Subject if an extension is required, explaining the reasons.

3. **Data Access and Portability**

    a. Provide a secure method for delivering personal data, such as encrypted email or secure portals.
    b. Ensure data is provided in a structured, commonly used, and machine-readable format (e.g., JSON, CSV).

4. **Data Rectification and Erasure**

    a. Update inaccurate or incomplete data in systems and backups.
    b. Permanently delete data unless retention is required for legal or regulatory purposes.

5. **Restriction and Objection**

    a. Temporarily suspend processing activities where applicable.
    b. Cease processing for direct marketing purposes if an objection is raised.

Step 4: Notification and Documentation

1. **Notification to Data Subjects**

    a. Confirm completion of the request and provide a summary of actions taken.
    b. In the case of rejection, provide reason and details.

2. **Escalation Process**

    a. If the Data Subject is dissatisfied with the resolution, provide guidance on how to escalate:

        i. Internal escalation to the Data Protection Officer (DPO).
        ii. External escalation to the Supervisory Authority (e.g., SDAIA NDMO).

3. **Internal Reporting**

    a. Document all actions taken in response to the request.
    b. Maintain a record of communications with the Data Subject for audit purposes.

Step 5: Monitoring and Improvement

1. **Performance Metrics**

    a. Monitor the following key metrics to ensure compliance and efficiency:

        i. Number of requests received, processed, and resolved.
        ii. Average response time for each type of request.
        iii. Number of escalations or complaints.

2. **Audits and Reviews**

    a. Conduct periodic audits to verify the effectiveness of the process and compliance with SDAIA NDMO and PDPL.

3. **Training and Awareness**

    a. Provide regular training for employees on handling Data Subject requests and protecting personal data.

4. **Process Optimization**

    a. Analyze trends in Data Subject requests to identify recurring issues and improve data handling practices.

5. Governance and Oversight

1. **Data Protection Officer (DPO)**

    a. Oversee the management of Data Subject requests and ensure compliance with regulations.
    b. Serve as the primary point of contact for Data Subjects and the Supervisory Authority.

2. **Data Governance Organization (DGO)**

    a. Ensure alignment of policies and procedures with SDAIA NDMO and PDPL.
    b. Monitor compliance through regular reporting and review.

3. **Senior Management**

    a. Approve updates to processes and ensure adequate resources for managing Data Subject rights.

6. Integration with Other Processes

This process is closely linked with:

1. **Data Breach Notification Process**

    a. Notify Data Subjects of breaches affecting their personal data.

2. **Notice and Consent Management**

a. Ensure Data Subjects are informed of their rights and provide clear mechanisms for exercising them.

7. Record-Keeping

1. **Documentation Requirements**

    a. Maintain detailed records of all Data Subject requests, including:

        i. Nature of the request.
        ii. Date of receipt and resolution.
        iii. Actions taken and communication with the Data Subject.

2. **Retention Period**

    a. Retain records for at least **5 years**, in compliance with SDAIA NDMO and PDPL requirements.

8. Penalties for Non-Compliance

Failure to comply with Data Subject rights management requirements may result in:

1. **Regulatory Penalties**

    a. Fines imposed by the Supervisory Authority (e.g., SDAIA NDMO).

2. **Reputational Damage**

    a. Loss of trust among Data Subjects and other stakeholders.

3. **Legal Liability**

    a. Legal actions from Data Subjects for damages incurred.