Notice of Personal Data Protection, Data Privacy, and Consent Management Process

Saudi Commission for Health Specialties (SCFHS)

Date: 02/12/2024

1. Objective

To establish a structured and compliant approach for creating, managing, and maintaining notices related to personal data protection and data privacy, while ensuring proper consent management in line with SDAIA NDMO, PDPL, and applicable regulations.

2. Scope

This process applies to all personal data collected, processed, or stored by the SCFHS, covering employees, customers, vendors, and other Data Subjects. It ensures compliance with SDAIA NDMO, PDPL, and other relevant regulations regarding notices and consent.

3. Definitions

1. **Personal Data**

   Any information related to an identified or identifiable individual (Data Subject).

2. **Data Subject**

   An individual whose personal data is processed by the SCFHS.

3. **Notice of Personal Data Protection**

   A document provided to Data Subjects, explaining how their personal data is collected, used, shared, and protected.

4. **Consent**

   A freely given, specific, informed, and unambiguous indication of the Data Subject's agreement to the processing of their personal data.

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

   The designated individual responsible for overseeing compliance with data protection laws.

4. Process Steps

Step 1: Drafting and Updating Privacy Notices

1. **Privacy Notice Requirements**

    a. Clearly define the purpose and legal basis for data processing (e.g., performance of a contract, consent, legal obligation).
    b. Specify the types of personal data collected (e.g., name, contact details, health data).
    c. Describe how the data will be used, shared, and stored.
    d. Include the rights of Data Subjects under PDPL, such as access, rectification, erasure, and objection.
    e. Provide the contact details of the DPO for queries or complaints.

2. **Periodic Review and Updates**

    a. Review privacy notices annually or when there are significant changes in data processing activities.
    b. Ensure updates are communicated to Data Subjects through appropriate channels (e.g., email, website).

3. **Multi-Channel Availability**

    a. Make privacy notices available through multiple channels, including the SCFHS's website, mobile apps, and physical locations, where applicable.

Step 2: Consent Management

1. **Obtaining Consent**

    a. Use clear and concise language to request consent.
    b. Provide Data Subjects with an option to opt-in or opt-out of specific data processing activities (e.g., marketing communications, data sharing with third parties).
    c. Obtain explicit consent for processing sensitive personal data (e.g., health or financial information).

2. **Recording Consent**

    a. Maintain detailed records of consent, including:

        i. Date and time consent was obtained.
        ii. Method of consent (e.g., electronic, written).

iii. Purpose(s) for which consent was given.

3. **Withdrawing Consent**

   a. Allow Data Subjects to withdraw consent at any time through simple and accessible means (e.g., website forms, customer support).
   b. Ensure that withdrawal of consent is promptly recorded and honoured.

Step 3: Communicating Privacy Practices

1. **Transparency and Accessibility**

   a. Ensure privacy notices are easy to understand and accessible in multiple languages, if applicable.
   b. Provide links to privacy notices in all forms or platforms where personal data is collected (e.g., online registration forms, physical contracts).

2. **Awareness Campaigns**

   a. Conduct regular awareness campaigns to inform employees, customers, and other stakeholders about privacy policies and consent management.

Step 4: Monitoring and Compliance

1. **Regular Audits**

   a. Conduct periodic audits to ensure privacy notices and consent mechanisms comply with SDAIA NDMO, PDPL, and any applicable international regulations (e.g., GDPR).
   b. Verify that all personal data processing activities align with the purposes stated in privacy notices.

2. **Compliance Monitoring**

   a. Track compliance with consent management practices through system logs and consent databases.
   b. Investigate and address any deviations from established processes.

Step 5: Handling Data Subject Requests Related to Notices and Consent

1. **Right to Information**

   a. Respond to Data Subject requests for access to privacy notices or consent records within the timelines specified by PDPL.

2. **Dispute Resolution**

    a. Address complaints or disputes related to privacy notices or consent handling through the DPO or a designated grievance mechanism.

5. Governance and Oversight

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

    a. Oversee the creation, maintenance, and dissemination of privacy notices.
    b. Monitor compliance with consent management practices.

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

    a. Ensure that privacy notices meet legal and regulatory requirements.
    b. Act as the point of contact for all Data Subject queries related to notices and consent.

3. **Senior Management**

    a. Review and approve updates to privacy notices and consent management processes.

6. Integration with Data Subject Rights

1. This process aligns with the SCFHS's Data Management and Personal Data Protection Policy, including:

    a. Right to Be Informed

    Data Subjects must receive clear and comprehensive privacy notices.

    b. Right to Consent

    Data Subjects must be allowed to provide and withdraw consent for data processing activities.

    c. Right to Rectification and Erasure

    Enable Data Subjects to request corrections or deletions if their data has been processed without proper consent or in contradiction to the privacy notice.

7. Record-Keeping

1. Maintain comprehensive records of:

    i. Versions of privacy notices issued, including timestamps.
    ii. Consent records, detailing when, how, and for what purpose consent was obtained.
    iii. Data Subject requests related to privacy notices and consent.

2. Retain records for a minimum of 5 years or as required by applicable regulations.

8. Tools and Technologies

1. **Consent Management Platforms (CMPs)**

    For managing, storing, and tracking Data Subject consent.

2. **Data Mapping Tools**

    To track personal data usage and ensure alignment with stated privacy policies.

3. **Customer Relationship Management (CRM) Systems**

    To manage Data Subject preferences and communication records.

9. Penalties for Non-Compliance

Failure to comply with privacy notice and consent management requirements may result in:

a. Administrative fines imposed by SDAIA NDMO or other authorities.
b. Reputational damage and potential legal liabilities.