Data Leak Notification Process

Saudi Commission for Health Specialties (SCFHS)

Date: 01/12/2024

1. Objective

To establish a robust and compliant process for identifying, managing, and notifying data leaks in line with SDAIA NDMO and PDPL requirements. This ensures the protection of personal data, adherence to privacy regulations, and safeguarding the rights of Data Subjects.

2. Scope

This process applies to all personal data processed, stored, or transmitted by the entity, ensuring compliance with applicable regulations, including SDAIA NDMO and PDPL.

3. Definitions

Data Leak

Unauthorized access, disclosure, or loss of personal data, compromising confidentiality, integrity, or availability.

Data Subject

An individual whose personal data is processed by the entity.

Data Protection Officer (DPO)

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

Supervisory Authority

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

4. Process Steps

Step 1: Identifying and Reporting Data Leaks

1. **Detection Mechanisms**

    a. Monitor systems for unusual activity using tools such as Data Loss Prevention (DLP) software and intrusion detection systems (IDS).
    b. Enable real-time alerts for unauthorized data access or transfers.
    c. Conduct regular audits to identify potential vulnerabilities.

2. **Internal Reporting**

    a. Employees must report suspected data leaks immediately to the Data Protection Officer (DPO) or via the SCFHS incident reporting system.
    b. Include key details such as the nature of the incident, data involved, and potential risks.

3. **Initial Assessment**

    a. The DPO, in collaboration with Information Security, must assess the severity of the suspected data leak.
    b. Categorize the leak (e.g., minor, significant, or critical) based on the nature and volume of data involved.

Step 2: Containment and Mitigation

1. **Immediate Actions**

    a. Isolate affected systems to prevent further data loss.
    b. Revoke access to compromised accounts or endpoints.
    c. Patch security vulnerabilities, if identified.

2. **Data Recovery**

    a. Restore any compromised data from secure backups.
    b. Validate the integrity of recovered data.

3. **Communication to Internal Stakeholders**

    a. Notify senior management and the Data Governance Department to oversee compliance with data protection policies.

Step 3: Risk Assessment and Impact Analysis

1. **Assess Risks to Data Subjects**

    a. Determine the type of personal data involved (e.g., sensitive, financial, medical).
    b. Evaluate the potential harm to Data Subjects, including identity theft, financial loss, or reputational damage.

2. **Root Cause Analysis**

    a. Investigate the root cause of the data leak.
    b. Document findings and corrective actions.

Step 4: Notifying the Supervisory Authority

1. **Mandatory Notification Timeline**

    a. Notify SDAIA NDMO or the relevant authority **within 72 hours** of becoming aware of a data leak, if the leak poses a significant risk to Data Subjects.

2. **Contents of Notification**

    a. Nature of the data leak and its root cause.
    b. Categories and approximate number of Data Subjects affected.
    c. Actions taken to mitigate risks.
    d. Contact details of the Data Protection Officer.

3. **Regular Updates**

    a. Provide periodic updates to the Supervisory Authority if the investigation or mitigation actions are ongoing.

Step 5: Notifying Data Subjects

1. **Criteria for Notification**

    a. Notify affected Data Subjects if the data leak poses a **high risk** to their rights or freedoms (e.g., sensitive data breach, financial risk).

2. **Notification Content**

    a. A clear explanation of the data leak and its potential impact.
    b. Recommendations for mitigating risks (e.g., changing passwords, monitoring financial accounts).
    c. Contact information for further assistance (e.g., DPO or customer service).

3. **Preferred Communication Channels**

    a. Use secure and reliable channels such as email, SMS, or physical mail, depending on the urgency and sensitivity of the notification.

Step 6: Remediation and Lessons Learned

1. **Incident Closure**

    a. Document all actions taken during the incident response.
    b. Submit a final report to the Supervisory Authority and senior management.

2. **Process Improvement**

    a. Update policies, procedures, and systems to prevent recurrence.
    b. Conduct a post-incident review and integrate lessons learned into the SCFHS data protection framework.

3. **Employee Training**

    a. Enhance training and awareness programs for employees on identifying and reporting data leaks.

5. Governance and Oversight

- **Data Governance Organization (DGO)**:

    a. Oversee compliance with personal data protection regulations.
    b. Ensure that policies, processes, and procedures align with SDAIA NDMO and PDPL requirements.

- **Data Protection Officer (DPO)**

    a. Act as the primary point of contact for data protection compliance and incident management.
    b. Ensure that the rights of Data Subjects are respected throughout the process.

- **Compliance Monitoring**

    a. Conduct regular audits and assessments to ensure ongoing compliance with SDAIA NDMO and PDPL.

6. Managing Data Subject Rights

1. The process for managing data leaks must align with the SCFHS established procedures for handling Data Subject rights, including:
    a. Right to be informed of data leaks affecting their personal data.
    b. Right to access details about the incident and measures taken.
    c. Right to request rectification of any incorrect or incomplete data.

7. Record-Keeping

1. Maintain detailed records of all data leaks, including:
    a. The nature of the incident.
    b. Notifications sent to the Supervisory Authority and Data Subjects.
    c. Actions taken to mitigate risks.
2. Retain records for at least **5 years**, in line with regulatory requirements.

8. Penalties for Non-Compliance

Failure to notify the Supervisory Authority or Data Subjects within the stipulated timeframe or to follow this process may result in:

a. Administrative fines imposed by SDAIA NDMO.
b. Reputational damage and legal liability.