مركز حماية البيانات الشخصية
PDPC
Personal Data Protection Center

# TEMPLATE: BREACH NOTIFICATION TO THE PDPC

Personal Data Protection Center

Version 1.1. - 5 January 2025

# Table of Contents

## 1. Identification of the Notifying Party and Contact Details

| | |
|---|---|
| **Name of Entity / Individual** | **[Company / Organization / Individual Name]** |
| **Sector** | **☐ Public Sector** **☐ Private Sector** **☐ Non-Profit Organization (NPO)** |
| **Official Correspondence Email Address** | *[Official Email Address]* |

### a) Notification Prepared and Submitted By

*(Select and complete as applicable)*

☐ Controller/ Processor

☐ Processor

- **Notification Submission Contact Details**

  - **Name:** [Name and Surname]
  - **Position / Title:**

    ☐ Data Protection Officer (DPO)

    ☐ Other Position/Title (please specify): _____
  - **Email Address:** [Email]
  - **Phone Number:** [Phone]

### b) Data Protection Officer Contact Details

*(To be completed only where the Data Protection Officer is **not** the contact person identified above)*

- **Name:** [Name and Surname]
- **Email Address:** [Email]
- **Phone Number:** [Phone]

## 2. Particulars of the Personal Data Breach

### a. Notification Status

- **Notification Type:**
  ☐ Initial Notification ☐ Follow-Up / Updated Notification
- **Reference Number (if applicable):** _____

### b. Key Dates and Timeline

- **Date and Time of Occurrence of the Breach (if known):**
  DD / MM / YYYY – HH:MM
  *(If the exact time is unknown, provide the estimated period.)*
- **Date and Time the Breach Was Detected:**
  DD / MM / YYYY – HH:MM
- **Date and Time the Controller-Processor/ Processor/ Data Protection Officer Became Aware of the Breach:**
  DD / MM / YYYY – HH:MM

**Note:**

**For the purposes of breach notification, the following distinctions apply:**

- **Occurrence:** refers to the incident itself, including what happened and the date and time at which it occurred, where known.
- **Detection (factual/technical event)**: refers to the point at which the incident was first identified, flagged, or suspected through technical controls, staff reports, or third-party notifications/ It can be **preliminary, partial, or unconfirmed**.
- **Awareness (legal threshold):** refers to the point at which the controller or processor has sufficient information to reasonably determine that a personal data breach has occurred. The statutory notification period of seventy-two (72) hours commences from this point, in accordance with the PDPL and its Executive Regulation.

## c. Detection by a third party (if applicable)

- **Was the breach detected by a third party?** ☐ Yes ☐ No

If yes, kindly provide the following details and attach supporting documentation (e.g. notification email, report):

- **Name of the Third Party:**
- **Email of the Third Party:**
- **Date and Time the Third Party Detected the Breach:** DD / MM / YYYY – HH:MM
- **Date and Time the Third Party Notified the Controller:** DD / MM / YYYY – HH:MM

## d. Information about the source of the data breach

*(Tick as many boxes as maybe applicable)*

| Physical / Organizational Causes | Cyber / Technical Causes |
|---|---|
| ☐ **Loss or theft of documents or devices**<br>☐ **Insecure storage or improper disposal**<br>☐ **Accident or human error**<br>☐ **Negligence**<br>☐ **Sabotage**<br>☐ **Other (specify):**<br>_____ | ☐ **Cyber Attack**<br>☐ **Malware**<br>☐ **Social engineering**<br>☐ **Denial of Service (DoS-DDoS)**<br>☐ **Ransomware**<br>☐ **Brute-Force Attack**<br>☐ **Other (specify):**<br>_____ |
| **Elaborate your answer:**<br><br>***(Example for guidance purposes only)***<br><br>The breach resulted from a phishing attack in which an employee received a fraudulent email impersonating a trusted service provider. The employee inadvertently disclosed login credentials, which were subsequently used by an unauthorized third party to access an internal system. The access was limited to a specific user account and did not involve system-wide compromise. The breach was detected through abnormal login activity identified by security monitoring tools, after which access was immediately restricted and credentials were reset. | |

## e. Security criteria affected from the data breach

*(Tick as many boxes as maybe applicable)*

| | | |
|---|---|---|
| ☐ Data confidentiality | ☐ Data integrity accessibility | ☐Data availability / |
| **Elaborate your answer:** | | |

## f. Method of Detection

| |
|---|
| Describe **how the breach was detected**, including monitoring systems, internal controls, or third-party notifications: _____ |
| **(Supporting documents may be annexed)** |

## g. Categories of personal data affected by the data breach

*(Tick as many boxes as maybe applicable)*

| Personal Data | Sensitive Personal Data |
|---|---|
| ☐ Contact Data | ☐ Health data |
| ☐ Location Data | ☐ Biometric Data |
| ☐ Customer Transaction | ☐ Children's Data |
| ☐ Professional or employment data | ☐ Financial Data |
| ☐ Other (specify): _____ | ☐ Other (specify): _____ |
| **Elaborate your answer:** | |

## h. Number of data subjects and records affected by the data breach

| |
|---|
| Number of Data Subjects/ Personal Data Records Affected: _____<br><br>*(If the numbers provided are estimates, please indicate this and briefly explain why exact figures are not available at the time of notification.)* |
| **Elaborate your answer:** |

## i. Data subject groups affected by the data breach and the effects on them

*(Tick as many boxes as may be applicable)*

| Affected Data Subject Groups | Potential Impact on Data Subjects |
|---|---|
| ☐ Staff<br>☐ Users<br>☐ Subscribers / Members<br>☐ Students<br>☐ Customers and potential clients<br>☐ Patients<br>☐ Children<br>☐ Vulnerable individuals<br>☐ Not yet determined | ☐ Loss of control over personal data<br>☐ Identity misuse or fraud<br>☐ Discrimination<br>☐ Restriction of rights<br>☐ Fraud<br>☐ Financial loss<br>☐ Reputational harm<br>☐ Compromise of personal data security / not clear for me – because security is already compromised |
| ☐ Other (Specify):<br>_____ | ☐ Other (Specify):<br>_____ |
| **Elaborate your answer:** | |

## 3. Particulars of the Personal Data Breach

### a. Timeliness of Notification

If more than seventy-two (72) hours have elapsed between the date and time of awareness of the breach and the submission of this notification, please provide a detailed explanation for the delay.

*(Applicable to initial notifications only.)*

**Explanation:**

### b. Communication with Data Subjects

In accordance with the PDPL & its Executive Regulation, data subjects shall be notified within **three (3) working days** from the date of notifying the PDPC of the breach or violation, and of the security measures taken, using the communication method agreed upon at the time of data collection.

Has the personal data breach been communicated to the affected data subjects?

☐ Yes, notification has been completed.

☐ Notification is currently in progress.

☐ No, notification has not yet been made.

**If not completed, please explain the reason and the expected timeframe for communication:** _____

### c. Date of Communication to Data Subjects

**Date of communication made or scheduled:**

**DD / MM / YYYY**

### d. Method of Communication

Provide details of the communication method(s) used or planned to notify data subjects (e.g. SMS, email, telephone call, secure electronic link), in accordance with the method designated for data processing purposes.

*(Where applicable, attach a sample copy of the communication.)*

### e. Channels for Data Subject Inquiries

| |
|---|
| Indicate the communication channels made available to enable data subjects to obtain further information about the breach (e.g. dedicated webpage, hotline, email address, call center). |
| **Explanation:** |

### f. Notification of Other Domestic Authorities or Institutions

| |
|---|
| Have any domestic authorities or institutions been informed of the breach, or is there an intention to inform them?<br><br>(e.g. supervisory or inspection bodies)<br><br>☐ Yes ☐ No |
| If yes, please specify the authority or institution, the reason for notification, and the date of communication.<br>*(Attach supporting documents, where applicable)* |

### g. Notification of Foreign Authorities or Institutions (if applicable)

| |
|---|
| Have any foreign data protection authorities or relevant institutions been informed of the breach, or is there an intention to inform them?<br><br>☐ Yes ☐ No |
| If yes, please provide details of the authority or institution, the legal basis for notification, and the date of communication.<br><br>*(Attach supporting documents, where applicable.)* |

## 4. Potential Consequences of the Data Breach

### a. Potential Impact on Data Subjects

This section assesses the **likelihood and severity of adverse effects** on data subjects resulting from the personal data breach.

In determining the level of potential impact, the following factors should be taken into account, as applicable:

- The **nature and type of the breach**;
- The **cause and circumstances** of the breach;
- The **categories and sensitivity of the personal data affected**;

- The **categories of data subjects concerned**; and
- The **mitigation measures implemented or planned** to reduce adverse effects.

Please indicate the **overall severity of the potential impact** on data subjects:

| Severity Level | Description |
|---|---|
| ☐ **Very High** | Data subjects may suffer severe and irreversible consequences or impacts that cannot reasonably be mitigated (e.g. inability to work, long-term psychological or physical harm). |
| ☐ **High** | Data subjects may face serious consequences that require significant effort to overcome (e.g. financial loss, employment impact, legal proceedings, deterioration of health). |
| ☐ **Medium** | Data subjects may experience negative effects that can be mitigated with reasonable effort or cost (e.g. stress, additional expenses, inconvenience, minor physical effects). |
| ☐ **Low** | Data subjects may experience limited or minor adverse effects that are easily manageable (e.g. temporary distress or inconvenience). |
| ☐ **Not yet known** | The potential impact cannot yet be determined at the time of notification. |

## b. Potential Impact on the Organization

Please assess the **impact of the breach on the organization's operations, services, and ability to function**:

| Severity Level | Description |
|---|---|
| ☐ **Very High** | Complete inability to provide services or perform core operational functions. |
| ☐ **High** | Inability to provide critical or essential services. |
| ☐ **Medium** | Reduced efficiency, operational disruption, or loss of control in certain activities or services. |
| ☐ **Low** | No material impact on service delivery or operational control. |

| | |
|---|---|
| ☐ **Not yet known** | The impact cannot yet be fully assessed. |

## 5. Measures Taken and Planned

### a) Preventive Measures in Place Prior to the Breach

Please indicate the **technical and organizational measures** that were implemented **before the occurrence of the breach** to prevent or reduce the likelihood of such incidents.

| Technical Measures | Organizational Measures |
|---|---|
| • … | • … |
| • … | • … |
| • … | • … |
| **Explanation:** | **Explanation:** |
| *(Supporting documents may be annexed, where applicable)* | |

### b) Remedial and Corrective Measures Taken or Planned After the Breach

Please describe the **technical and organizational measures** taken or planned **in response to the breach**, including measures aimed at:

- Containing the incident;
- Eliminating or mitigating adverse effects; and
- Preventing recurrence.

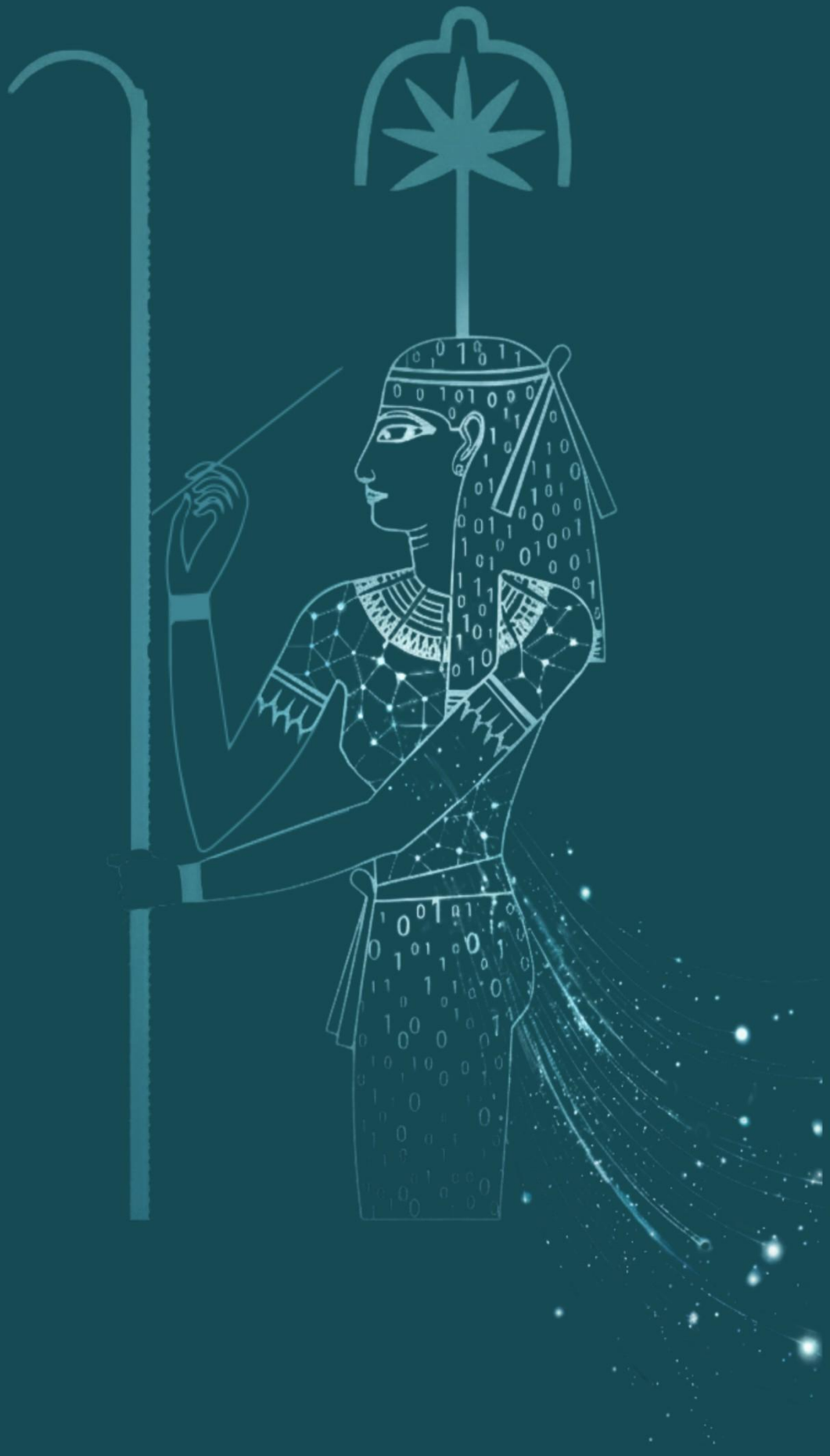
Where applicable, indicate the **expected completion timeline**.

| Technical Measures | Organizational Measures |
|---|---|
| • … | • … |
| • … | • … |
| • … | • … |

| | |
|---|---|
| **Explanation:** | **Explanation:** |
| *(Supporting documents may be annexed, where applicable)* | |

## 6. National Security Considerations

| |
|---|
| Is the personal data breach or violation associated, whether directly or indirectly, with national security considerations or with entities entrusted with national security responsibilities?<br><br>☐ Yes ☐ No |
| If yes, please provide the following information:<br><br>I. Describe the connection between the breach or violation and national security considerations _____<br>II. Specify the volume of personal data affected and provide an assessment of the resulting or potential damage _____ |



@pdpceg

info@pdpc.gov.eg