HUMANICA PUBLIC COMPANY LIMITED

Personal Data Breach Procedure

Document Details

Document No.	PDPA-PC-0901
Version	2.0
Document Name	Personal Data Breach Procedure
Enforcement Date	10th of July 2023

Documentation of Changes

Version	Operator	Enforcement Date	Details
1	PDPA Project Working Team	31st of May 2022	Document Creation
2	DPO	10th of July 2023	Revise the Procedure for Personal Data Breach.

Table of Contents

1. Objective

Objectives of establishing procedures for responding to incidents that impact the security of personal data are as follows:

- Clearly define roles and responsibilities of relevant parties involved in incident response related to the security of personal data of the company.
- Define operational guidelines for handling incidents that impact the security of personal data.
- Explain communication and internal management within the organization and with external individuals regarding incidents that impact the security of personal data.
- Provide contact details for responsible personnel and external departments.

All employees involved in this should be aware of these procedural steps in order to handle incidents that may impact the security of personal data.

Contact information and other relevant details should be reviewed and updated at least once a year. Any changes to the contact list or other related details that occur outside of the scheduled reviews should be promptly notified to dpo@humanica.com

All personal data mentioned in this document is part of the incident response process that impacts the security of personal data. It will be used for the purpose of managing data security incidents and is subject to the Personal Data Protection Act of 2562.

2. Scope

Incidents that impact the security of personal data or result in privacy breaches involving the collection, use, and disclosure of personal data by the company.

3. Definitions

No.	Terms	Definitions
1	Company	Humanica Public Company Limited and subsidiary companies
2	Subsidiary companies	The list of company names follow this link https://www.humanica.com
3	Data processing	Any operation or set of operations performed on personal data or sets of personal data, whether by automated means or not. This includes collecting, recording, organizing, structuring, storing, altering, modifying, retrieving, consulting, using, disclosing by transmission, disseminating, or any other action that enables data to be ready for use, arranged, combined, restricted, deleted, or destroyed.
4	Personal Data	Means information related to a natural person which can be used to identify such person whether directly or indirectly. This excludes information relating to deceased persons.
5	Sensitive Data	Means personal data relating to nationality, race, political opinions, religious, philosophical, or spiritual beliefs, sexual behavior, criminal records, medical records, disability, trade union information, genetic data, biometric data (such as face scanning, iris scanning, or fingerprints) or other information which similarly impacts the data subjects as determined by the Personal data Protection Committee.
6	Data Subject	Any individual whose data allows for the identification of their identity, whether directly or indirectly.
7	Data Owner	The individual who has direct responsibility for that information. They may obtain the data directly from the data subject or be the creator of the data themselves. The data owner has the responsibility to determine the classification level of the data and the level of risk associated with various sets of personal data.
8	Data Custodian	The person assigned by the data owner to maintain and secure the information in accordance with the confidentiality level of the data. Generally, the data custodian is a technology officer or IT personnel.
9	Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure and access to personal data.

3.1 Responsibility

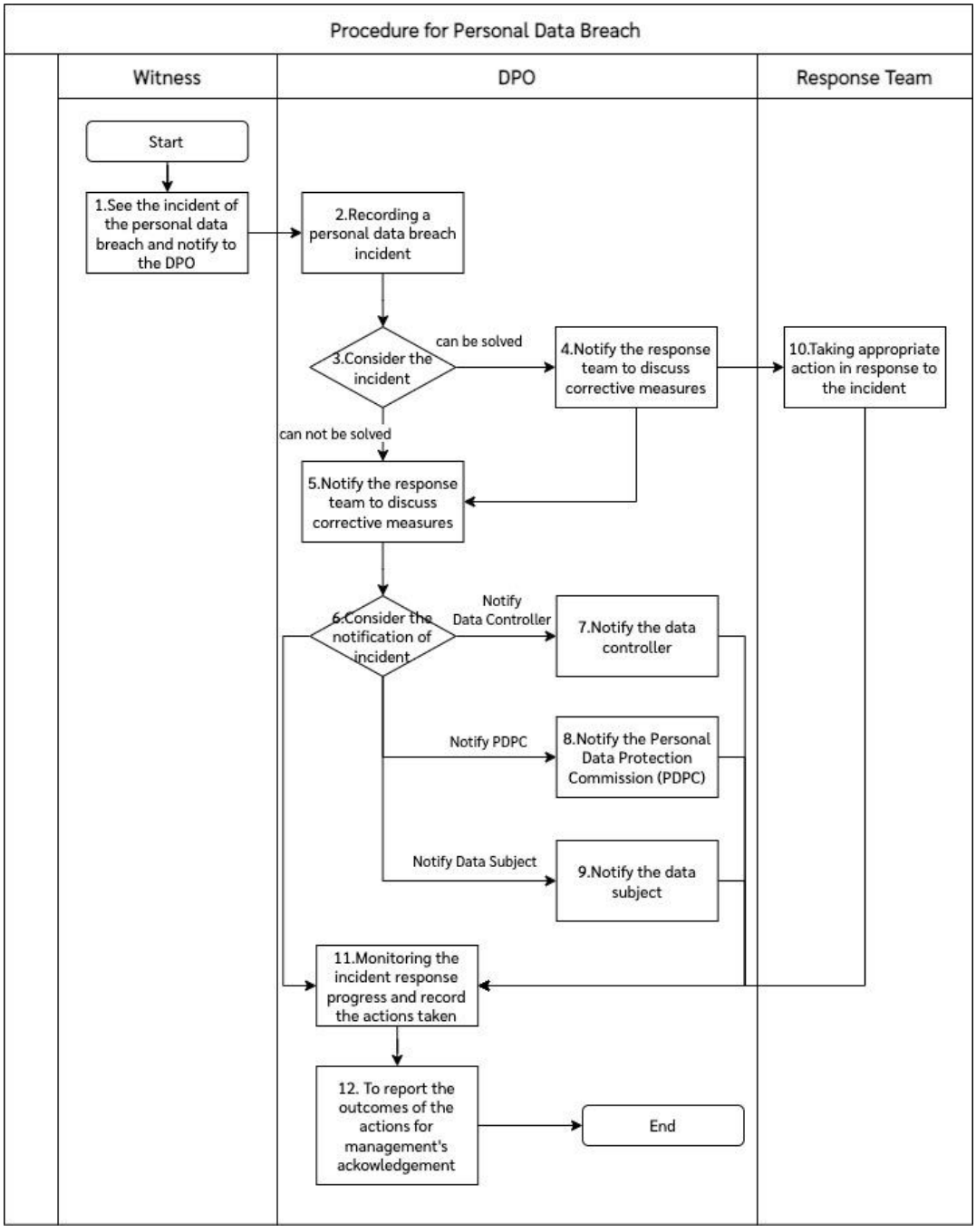
- All employees are responsible for promptly reporting incidents that may impact the security of personal data, taking into consideration the severity of the incident.
- All employees are responsible for reporting incidents that may impact the security of personal data to their superiors and the company's data protection officers, ensuring that they are informed of the incidents that may affect the security of personal data.

3.2 Reporting incidents that could impact the Personal Data Breach

- Any individual who accesses, uses, or manages the personal data of the company is responsible for reporting incidents that may impact the security of personal data, whether it involves data breaches or violations of the Personal Data Protection Act to the data protection officer at dpo@humanica.com**.**
- In the event of incidents that may impact the security of personal data or data breaches occurring or being discovered outside of regular working hours, they must be reported immediately as soon as possible taking into consideration the severity of the breach.
- Details of incidents that may impact the security of personal data or data breaches such as date, time, name of the reporter, nature of the data, and the number of individuals involved. Should be recorded in a Personal Data Breach Register form if the data is related to personal data.
- All employees should be aware that non-compliance with the Personal Data Protection Act of 2562 may result in disciplinary action by the company.

4. Procedure for Personal Data Breach

The procedure for responding to incidents that impact the security of personal data is shown in the following diagram.



Details of the procedure as follows.

Process	Description
1. See the incident of the personal data breach and notify to the DPO	When an employee or individual witnesses an event that impacts the security of personal data they should notify the DPO through the channels specified in the personal data protection policy.
2. Recording a personal data breach incident	The DPO should record the details of incident in the Personal Data Breach Register form, including the following information: ▪ The scope of impact on IT infrastructure including computers, network systems, information devices, and the situation surrounding the incident. ▪ Data assets including personal data that may be at risk or have been compromised. ▪ Time of the occurrence of the incident. ▪ Business units affected and the extent of the impact. ▪ The extent of the risk and potential impact on the rights and freedoms of individuals whose personal data has been breached. ▪ Preliminary indications of the possible causes of the incident.
3. Consider the incident	Assess whether the personal data breach can be resolved or mitigated. ▪ If the incident can be resolved or mitigated, proceed with the steps outlined in step 4. ▪ If the incident cannot be resolved or mitigated, proceed with the steps outlined in step 5.
4. Notify the response team to discuss corrective measures	Notify the response team to discuss corrective measures for the personal data breach incident.
5. Notify the management regarding the incident	Notify the management about the personal data breach incident and provide initial management guidelines.
6. Consider the notification of incident	Consider the notification of incident to determine which organizations should be notified: ▪ In the case of notifying the data controller, proceed with step 7. ▪ In the case of notifying the Office of the Personal Data Protection Commission, proceed with step 8. ▪ In the case of notifying the data subjects, proceed with step 9. ▪ In the case no need to notify any organization, proceed with step 10.
7. Notify the data controller	In the case of personal data related to customer data, the DPO must notify the data controller of the incident and provide detailed information.

Process	Description
8. Notify the Personal Data Protection Commission (PDPC)	The DPO is responsible for assessing the personal data breach. If it is determined that there is a risk that may impact the rights and freedoms of individuals, the DPO must notify the Personal Data Protection Commission in accordance with the guidelines outlined in **5. Guidelines for Notifying the Personal Data Protection Commission (PDPC)**.
9. Notify the data subject	The DPO should assess the personal data breach incident, and if it is determined that the breach poses a high risk to the rights and freedoms of individuals, the DPO must notify the data subjects in accordance with the guidelines outlined in **6. Guidelines for Notifying Data Subjects**.
10. Taking appropriate action in response to the incident	The incident response team is taking action to respond to the personal data breach, with the aim of containing the incident and preventing its escalation.
11. Monitoring the incident response progress and record the actions taken	The DPO monitors the incident response progress and records the outcomes of the corrective actions taken.
12. To report the outcomes of the actions for management's acknowledgment.	The DPO reports the outcomes of the actions to management for their acknowledgment.

5. Guidelines for Notifying the Personal Data Protection Commission (PDPC)

In the event that the company is the data controller involved in a personal data breach incident, the company is responsible for notifying the Personal Data Protection Commission via email at pdpc.dpo@mdes.go.th**.** The subject of the email should clearly state "Personal Data Breach Notification" and indicate the confidentiality level of the email as "Confidential."

5.1 Decision to notify the Personal Data Protection Commission (PDPC)

The Personal Data Protection Act of 2562 stipulates that in the event of a personal data breach the data controller must notify the Personal Data Protection Commission unless the breach poses no risk to the rights and freedoms of individuals. Therefore, the company must assess the level of risk before deciding whether to report the breach or not.

Factors to consider when assessing the potential impact on the rights and freedoms of individuals are as follows:

- Whether the personal data was encrypted
- If encrypted, the strength of the encryption used
- Whether it involves pseudonymous data and what level (e.g. whether personal identity can be derived from the breached data).
- The types of data breached e.g. names, addresses, financial details, biometric data.
- The volume of data involved
- The number of data subjects affected

- The nature of the breach e.g. theft, accidental destruction
- Any other relevant factors.

When conducting risk assessments, providing justifications and conclusions should be documented thoroughly and signed by the authorized personnel. The resulting risk assessment should include one of the following conclusions:

- Personal data breaches do not require reporting to the Personal Data Protection Commission.
- Personal data breaches must be reported exclusively to the Personal Data Protection Commission.
- Personal data breaches necessitate reporting to both the Personal Data Protection Commission and the affected data owners regarding the impact on rights and freedoms.

These conclusions may be subject to changes based on recommendations from the Personal Data Protection Commission and additional information discovered during the investigation of the personal data breach.

5.2 How to notify the Personal Data Protection Commission (PDPC)

If a decision to notify the Personal Data Protection Commission, the Personal Data Protection Act of 2562 requires data controllers to take action promptly within 72 hours of becoming aware unless there are justifiable reasons for the delay.

Notifying should be made through the appropriate secure communication method to the Personal Data Protection Commission, as indicated in the contact details specified in the *(Personal Data Breach Notification Form to Authority) PDPA-FM-0903-HMC-EN*. If reporting exceeds the 72 hour timeframe the reasons for the delay must be provided.

The company should receive a written acknowledgement from the Personal Data Protection Commission upon receipt of the data breach report including the date and time of notification.

Document regarding the personal data breach including its impact and remedial actions taken should be prepared as part of the incident response process that addresses the potential impact on the security of personal data.

6. Guidelines for Notifying Data Subjects

In case the company is the data controller involved it may be necessary to notify the personal data breach to the data subjects affected ensuring that they are informed of the impact on their rights and freedoms.

6.1 Decision to notify data subjects

According to the Personal Data Protection Act of 2562, it is stipulated that in the event of a personal data breach that poses a high risk to the rights and freedoms of individuals the data controller must notify it to the data subjects.

Risk assessment involves considering the factors that may impact the rights and freedoms of individuals, as outlined in section 5.1. If it is determined that there is a high risk, the data controller must notify it to the data subjects.

The company may be exempted from notifying the data subjects of the personal data breach under the following conditions:

- The company has implemented appropriate technical and organizational measures for data protection and applied them to the personal data involved in the breach.
- The company has taken post-breach measures that assure that the high risk to the rights and freedoms of individuals cannot be achieved.
- Notifying the data subjects is excessively difficult. The company will undertake public notification or alternative methods instead.

6.2 How to notify data subjects

When a decision is made to notify an incident to the data subjects whose personal data has been violated, the notification must be done without delay.

The notification to the data subjects who have been affected must clearly and easily explain the nature of the personal data breach, covering the following:

1) The description of the personal data breach should include the ability to specify the type and quantity of personal data involved, as well as record related processing activities.
2) Names and contact details of the company's data protection officers or alternative contacts for obtaining additional information.
3) Explanation of the impact resulting from the personal data breach.
4) Description of the measures implemented or proposed to address the personal data breach including appropriate remedial and mitigating measures.

Additionally, it is recommended to offer guidance to the data subjects whose personal data has been breached in order to minimize the risks associated with the data breach. This can be achieved by informing the affected data subjects about the incident through a Breach Notification Letter (PDPA-FM-0902-HMC-EN), email, or both, ensuring that they are properly informed.

7. List of Teams for Incident Response

Reference PDPA-RF-1501-HMC DPO and Contact Point

The roles and responsibilities of the incident response team.

7.1 Supervisor

- Making a decision to initiate an incident response plan or not.
- Gathering the incident response team.
- Overall management of the incident response team.
- Acting as a coordinator with other high-level committees and decision-makers.
- Serving as the final decision-maker in cases of conflicting opinions.

7.2 Secretary

- Facilitating the convenience of the incident response team.
- Coordinating internal resources within the operations center.
- Preparing for meetings, documenting actions, and making decisions.
- Summarizing the latest situation to team members upon their return to the operations center.
- Ensuring convenience in communication through email, telephone, fax, or other communication methods.
- Verifying external data.

7.3 Coordinator

- Access the incident location as quickly as possible.
- Assess the scope and impact of the incident.
- Compile a list of individuals directly involved in the incident and provide it to the response team.
- Coordinate with the response team continuously to provide additional information and answer any necessary questions for decision-making by the response team.

7.4 IT

- Provide information on issues related to information technology.
- Assist in evaluating the impact.

7.5 Business Operation

- Make decisions based on knowledge of business operations, products, and services.
- Summarize business-related issues for other team members.
- Assist in assessing potential impacts on the organization's customers.

7.6 Facilities Management

- Establish agreements regarding physical security and access to premises or assets.
- Procure and maintain security measures as necessary.

7.7 Health and Safety

- Assess the risks to life and property posed by the incident.
- Verify compliance with health and safety regulations.
- Coordinate with emergency services such as police, fire, and medical personnel.
- Consider environmental issues related to the incident.

7.8 HR

- Assess and provide recommendations on personnel policies and employment contracts.
- Assess and provide advice or feedback on the impact experienced by employees within the organization.
- Offer insights on disciplinary matters concerning employees.

7.9 BCM

- Provide advice on business continuity options.
- Implement a business continuity plan if necessary.

7.10 Corporate Communication

- Take responsibility for efficiently examining internal communications.
- Determine the frequency and content of external communications such as media.
- Establish guidelines for notifying affected parties such as customers and shareholders.

7.11 Legal

- Provide guidance to ensure compliance with relevant laws and regulatory frameworks.
- Evaluate the actual legal consequences and potential outcomes resulting from events and their impacts.

8. Related documents

No.	Document No.	Document Name
1	PDPA-FM-0904-HMC-EN	Personal Data Breach Register
2	PDPA-FM-0903-HMC-EN	Personal Data Breach Notification Form to Authority
3	PDPA-FM-0902-HMC-EN	Breach Notification Letter to Data Subjects
4	PDPA-RF-1501-HMC	DPO and Contact Point