

THE SOFTWARE PRACTICE PTE LTD	No of Pages	1 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

AMENDMENTS LOG

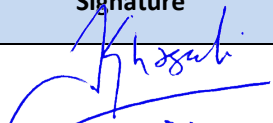
Revision History

Version	Date	Revision Author	Summary of Changes
1.0	10 June 2024	Edwin Soedarta DPO	First Release

Distribution

Name	Location
<i>All employees</i>	<i>Shared Folder</i>

Review & Approval

Name	Position	Signature	Date
Khasali M	Director		10 June 2024

THE SOFTWARE PRACTICE PTE LTD	No of Pages	2 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

Contents

AMENDMENTS LOG	1
RECORDS FOR DOCUMENT REVIEW	3
INTRODUCTION	4
PURPOSE	4
DEFINITIONS	4
RESPONSIBILITIES AND AUTHORITIES	5
PROCEDURES	5
1 IDENTIFY A BREACH	5
2 WHO DO THESE PROCEDURES APPLY TO?	6
3 WHAT TYPES OF DATA DO THESE PROCEDURES APPLY TO?	6
4 WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACH?	6
5 PROCEDURE FOR REPORTING PERSONAL DATA SECURITY BREACHES	6
6 PROCEDURE FOR MANAGING DATA SECURITY BREACHES	7
7 TRAINING & DEVELOPMENT	14
8 FORMS	14
9 ANNEX	14

THE SOFTWARE PRACTICE PTE LTD	No of Pages	4 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

INTRODUCTION

A data breach refers to an incident exposing personal data in an organization’s possession or under its control to the risks of unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. Data breaches often lead to financial losses and a loss of consumer trust for the organization. In addition, individuals whose personal data have been compromised (the “affected individuals”) could be at risk of harm or adverse impact if they do not take steps to protect themselves. Hence it is important for organizations to be accountable towards individuals by preventing and managing data breaches.

The organization is obliged under the Personal Data Protection Act (PDPA) to keep personal data safe and secure and to respond promptly and appropriately to personal data security breaches, and to make the appropriate notification(s) of the data breach. It is vital to take prompt action in the event of any actual, potential or suspected breaches of personal data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and potential financial, legal and reputational costs to the organization.

PURPOSE

The purpose of these procedures is to provide a framework for reporting and managing data security breaches affecting personal data held by the organization. These procedures supplement the organization’s data protection and information security policies which affirms its commitment to protect the privacy rights of individuals in accordance with PDPA and the Personal Data Protection (Notification of Data Breaches) Regulations.

DEFINITIONS

Sensitive Personal Data Any Personal Data which are considered likely to result in significant harm to an affected individual.

Examples:

- 1) Individual’s full name OR national identification number + any of the following: financial, medical, vulnerable person, private key to authenticate or authorize a record or transaction
- 2) Individual’s account information + any of the following: security/access code, password or answer to security question used to permit access to or use of an account

Note: To provide certainty on the data breaches that are notifiable, the [Personal Data Protection \(Notification of Data Breaches\) Regulations](#) provides the personal data that is deemed to result in significant harm to affected individuals if compromised in a data breach.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	5 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

RESPONSIBILITIES AND AUTHORITIES

The Top Management has the prime responsibility and approval authority for this procedure.

The Data Protection Committee is responsible for the investigation and response in the steps detailed below.

PROCEDURES

1 IDENTIFY A BREACH

1.1 A personal data breach is a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.2 What this means is that security incidents, perhaps caused by an IT error or loss of service, may not be a personal data breach. All personal data breaches will be security incidents, but not all security incidents will be personal data breaches. This Policy is concerned with the former not the latter.

1.3 Data breaches can be categorized in the following well-known information security principles:

- **Confidentiality breach** - where there is an unauthorized or accidental disclosure of, or access to, personal data
- **Availability breach** - where there is an accidental or unauthorized loss of access to, or destruction of, personal data
- **Integrity breach** - where there is an unauthorized or accidental alteration of personal data

1.4 A breach can be all three at the same time, or any combination of these.

1.5 Some of the most common ways in which Personal Data is breached is as follows:

- the disclosure of personal data to unauthorized individuals;
- loss or theft of equipment on which personal data is stored;
- loss or theft of paper records containing personal data;
- inappropriate access controls allowing unauthorized use of personal data;
- suspected breach of the organization’s IT security and Acceptable Use policies;
- attempts to gain unauthorized access to computer systems, e.g., hacking;
- records altered or deleted without authorization by the data “owner”;
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g., forcing of doors or filing cabinet containing personal data
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing personal data
- emails containing personal data sent in error to the wrong recipient.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	6 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

2 WHO DO THESE PROCEDURES APPLY TO?

These procedures apply to all users of personal data, including:

- any person who is employed by the organization or is engaged by organization who has access to personal data in the course of their employment or engagement;
- individuals who are not directly employed by the organization, but who are employed by the Data Intermediary (or subcontractors) as authorized by the organization and who have access to data in the course of their duties for the organization hereinafter.

3 WHAT TYPES OF DATA DO THESE PROCEDURES APPLY TO?

These procedures apply to:

- all personal data created or received by the organization in any format (including paper records), whether used in the workplace, stored on portable devices and media, hosted in cloud, transported from the workplace physically or electronically or accessed remotely;
- personal data held on all organization's IT systems

4 WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACH?

Personal data security breaches are managed by the Data Breach Management Team.

Data Breach Management Team	Designation
Team Lead	Director
Coordinator	DPO
Members	Data Protection Committee (DPC) Members
Technical Lead	IT Ops

5 PROCEDURE FOR REPORTING PERSONAL DATA SECURITY BREACHES

In the event of a breach of personal data, it is vital to ensure that it is dealt with immediately and appropriately to minimize the impact of the breach and prevent a recurrence. Refer to Annex B for the Drawer Plan.

If a staff / data intermediary becomes aware of an actual, potential or suspected breach of personal data, he/she must report the incident to the DPO or Director **immediately** both during office hours and outside office hours.

Refer to Annex A for the Possible Data Breach Scenarios

THE SOFTWARE PRACTICE PTE LTD	No of Pages	7 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

6 PROCEDURE FOR MANAGING DATA SECURITY BREACHES

The following five steps should be followed in responding to a data breach:

I-C-A-R-E
Step 1: Identification
Step 2: Containment
Step 3: Assessment
Step 4: Reporting (Notification)
Step 5: Evaluation

Step 1: Identification

- 6.1 The Data Breach Management Team shall gather relevant information about the data breach.
- Cause of the data breach and whether the breach is still ongoing
 - Number of individuals affected
 - Types of personal data involved
 - Systems, repositories affected
 - Whether help is required to contain the breach
 - The remediation action(s) that the organization has taken or needs to take to reduce any harm to affected individuals resulting from the breach.

The details of the incident shall be recorded in DPMP-PRO-03-F1 Data Breach Report to be maintained by the DPO and registered in DPMP-PRO-03-F2 Data Breach Record Log for tracking purposes.

Step 2: Containment

- 6.2 Once it has been established that a data breach has occurred, the organization needs to take immediate and appropriate action to contain the breach.
- 6.3 The Data Breach Management Team shall:
- Establish who within the organization needs to be made aware of the breach and inform them of what they are expected to do to contain the breach. The following immediate containment actions may be considered, where applicable:
 - Isolate the compromised system from the internet or network by disconnecting all affected systems
 - Re-route or filter network traffic, closing particular ports or mail servers
 - Prevent further unauthorized access to the system. Disable or reset the passwords of compromised user accounts
 - Isolate the causes of the data breach in the system, and where applicable, change the

THE SOFTWARE PRACTICE PTE LTD	No of Pages	8 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

- access rights to the compromised system
- Stop the identified practices that led to the data breach
- Establish whether the loss of data can be recovered and implement further action to minimize any harm caused by the data breach (e.g., recalling an email that has been accidentally sent or forwarded etc.)
- **The Data Breach Management Team may consider alerting the following bodies if they suspect that criminal acts have been perpetrated, as these bodies may also offer assistance in containing the data breach. The notification to these parties may be done without undue delay once the criminal act is suspected:**
 - **The Police, if criminal activity (e.g., hacking, theft, or unauthorized access by an intruder) is suspected, and to preserve evidence for investigation.**
 - **Cyber Security Agency of Singapore (CSA) through the Singapore Computer Emergency Response Team (SingCERT) for cyber incidents.**
- The Data Breach Management Team shall also be mindful of the requirements set out by respective sectoral regulations applicable to them for reporting of data breaches.

Step 3: Assessment

- 6.4 Upon containment of the data breach, the Data Breach Management Team shall conduct an in-depth assessment of the data breach, the success of its containment actions, or the efficacy of any technological / physical / administrative protection applied to the personal data involved in the breach.
- 6.5 Assessing the extent and likely impact of the data breach will help the organization identify and take further steps to limit the harm resulting from a data breach and prevent the recurrence of similar incidents.
- 6.6 An assessment of the extent of the data breach and whether it is likely to result in significant harm or impact to the affected individuals will also assist the organization in deciding whether to notify the PDPC and affected individuals.

For notifiable data breach as per the result of the assessment, the timeframes for notifying PDPC and affected individuals will thus commence from the time the DPO determines that the breach is a notifiable data breach.

Refer to Step 4 Notification for the summary of the data breach notification points.

- 6.7 In assessing the likely impact of the data breach, the Data Breach Management Team should consider the following:
- Context of the data breach:
 - In considering the context of a data breach, the organization should take into account factors such as the types of personal data involved, the individuals whose personal data have been compromised, and other contextual factors such as whether the personal data was publicly available before the data breach.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	9 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

- The disclosure of certain types of personal data, for example, national identification numbers, health records, financial information, user credentials may involve a risk of significant harm as compared to a disclosure of other types of personal data like names and email addresses.
- Certain individuals (e.g., vulnerable persons, minors) may also be at particular risk of significant harm. Significant harm could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation and other forms that a reasonable person would identify as a possible outcome of a data breach.
- Ease of identifying individuals from the compromised data
 - The ease with which an affected individual can be identified from the compromised data increases the likelihood of harm and impact to the individual. In general, the ease of identifying individuals from the compromised dataset increases with the number and uniqueness of identifiers in the dataset.
 - For example, it would be easier to identify individuals from a compromised dataset of records containing full names, national identification numbers, personal mobile phone numbers and email addresses, as compared to a dataset containing names and email addresses only.
- Circumstances of the data breach
 - The organization should consider the circumstances surrounding the data breach, such as whether the data was illegally accessed and stolen by those with malicious intent, which is more likely to result in significant harm to the affected individuals as compared to situations where the data was wrongly sent to recipients who have no malicious intent or use for the data.
 - The availability of the monitoring tools may provide access, authentication, encryption, audit logs which can assist the organization in determining how the data breach happened.
 - The organization should also consider if the personal data had been publicly accessible for a significant period of time before the organization became aware of the data breach.
 - The risks that the personal data had been accessed and used in ways that could result in harm increases with longer periods of time it was exposed.
- Conclude whether the data breach is unlikely or likely to result in significant impact or harm to the affected individuals.
- Consider, and if necessary, take further steps to reduce any potential harm to the affected individuals. For example, if the data breach involves the accidental disclosure of personal data to a trusted third party, the organization could take steps to request that the third party delete the personal data that was accidentally disclosed and secure the third party's compliance with its request. organization may also implement fixes to system errors/bugs to prevent further disclosure of/access to personal data; and
- Where a data breach is assessed to be likely to result in significant harm / impact to the individuals or of a significant scale (e.g., involves 500 or more individuals), the DPO shall

THE SOFTWARE PRACTICE PTE LTD	No of Pages	10 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

conclude that the data breach is notifiable to PDPC. When a data breach is assessed to be likely to result in significant harm / impact to the individuals, and applicable exceptions do not apply, affected individuals must also be notified after notification to PDPC.

Step 4: Reporting (Notification)

- 6.8 Depending on the outcome of assessment, the data breach may have to be notified to the PDPC and affected individuals.
- 6.9 DPO may also choose to voluntarily notify PDPC even if the breach is not mandatorily notifiable in case it needs timely guidance on the appropriateness of the remedial actions taken by the organization.
- 6.10 Data intermediaries (DI) engaged by the organization that process personal data on behalf of the organization shall be required to notify the organization of a data breach upon detection. This obligation shall be documented in the data processing agreement with the Data Intermediaries. Similarly, if our company is acting as the DI, the DPO shall inform the Data Controller of the breach upon detection without undue delay (no later than 24 hours).
- 6.11 Criteria for Data Breach Notification
1. If the data breach is likely to result in significant harm to an affected individual. Personal data that are considered likely to result in significant harm to an individual when compromised:
 - a. Individual's full name or national identification number (e.g., NRIC) + any of the following information: financial, medical, vulnerable person, private key to authenticate or authorize a record or transaction
 - b. Individual's account information + any of the following: security/access code, password or answer to security question used to permit access to or use of an account

To provide certainty on the data breaches that are notifiable, the [Personal Data Protection \(Notification of Data Breaches\) Regulations](#) provides the personal data that is deemed to result in significant harm to affected individuals if compromised in a data breach. Where a data breach involves any of the prescribed personal data, the organization will be required to notify the PDPC and the affected individuals of the data breach (where required).

2. If data breach meets the significant scale criteria. Where a data breach affects 500 or more individuals, the organization is required to notify the PDPC, even if the data breach does not involve any prescribed personal data in the [Personal Data Protection \(Notification of Data Breaches\) Regulations](#).

If an organization is unable to determine the actual number of affected individuals in a data breach, the organization should notify the PDPC when it has reason to believe that the number of affected individuals is at least 500. The organization may subsequently update the PDPC of the actual number of affected individuals when it is established.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	11 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

6.12 Upon determining that a data breach is notifiable, the organization must notify:

- **The PDPC as soon as practicable, but in any case, no later than 3 calendar days¹, and**
- **Where required, affected individuals after notifying the PDPC.**

6.13 In notifying the PDPC and the affected individuals (where required), the organization should take into consideration the following points:

Point 1: When to notify PDPC?

The DPO will notify the PDPC of a data breach that is:

- Of a significant scale (i.e., data breach involves personal data of 500 or more individuals); or
- Likely to result in significant harm or impact to the individuals to whom the information relates

Point 2: How soon does the DPO need to notify PDPC?

As soon as practicable, and in any case no later than 3 calendar days from the day it determines a notifiable data breach has occurred.

Point 3: How should the DPO notify PDPC?

Submit the notification at <https://eservice.pdpc.gov.sg/case/db>. For urgent notification of major cases, organization may also contact PDPC at +65 6377 3131 during office hours.

Point 4: What details does the DPO need to include in the notification to PDPC?

- Facts of the data breach
 - The date on which and the circumstances in which the organization first became aware that a data breach has occurred;
 - Information on how the notifiable data breach occurred;
 - The number of affected individuals affected by the notifiable data breach; and
 - The potential harm to the affected individuals as a result of the notifiable data breach.
- Data breach handling
 - A chronological account of the steps taken by the organization after the organization became aware that the data breach had occurred, including the results of its assessment that the data breach is a notifiable data breach;
 - Information on any actions, whether taken before or to be taken after PDPC notification, to eliminate or mitigate the potential harm, and to address or remedy failure or shortcoming that had caused or enabled the breach; and
 - Information on the plan to inform all or any affected individuals or the public of the notifiable data breach and how an effected individual may eliminate or mitigate any potential harm

¹As prescribed under the Personal Data Protection Act.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	12 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

- Contact details
 - Data Protection Officer (DPO) contact details that PDPC can contact for further information

Where specific information of the data breach is not yet available, the DPO should send an interim notification within 3 calendar days based on the most accurate information available at the point in time that the notification is made.

Where the organization does not intend to notify any affected individual, the PDPC notification must additionally specify the grounds (whether under the PDPA or other written law) for not notifying the affected individual.

Point 5: When to notify affected individuals?

Where required (**refer to point #9 for exceptions**), the organization should notify the affected individuals of a data breach that is likely to result in significant harm or impact to them as soon as practicable, **on or after notifying the PDPC²**.

Point 6: How soon does the organization need to notify affected individuals?

On or after notification to PDPC.

Point 7: How should the organization notify affected individuals?

The organization should adopt the most effective way to reach out to them, taking into consideration the urgency of the situation and number of individuals affected (e.g., emails, telephone, social media).

Notification should be simple to understand, specific and provide clear instructions on what individuals can do to protect themselves.

Point 8: What details does the organization need to include in the notification to affected individuals?

- Facts of the data breach
 - The circumstances in which the organization first became aware that a notifiable data breach has occurred; and
 - The personal data or classes of personal data relating to the affected individual affected by the notifiable data breach.
- Data breach management and remediation plan
 - Potential harm to the affected individual as a result of the notifiable data breach;
 - Information on any action by the organization, whether taken before or to be taken after the organization notifies the affected individual to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach, and to address or remedy any failure or shortcoming that had caused or enabled the data breach

²As prescribed under the Personal Data Protection Act.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	13 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

- Steps that the individuals may take to eliminate or mitigate any potential harm as a result of the data breach, including preventing the misuse of the affected individual's personal data affected by the data breach
- Contact details
 - Contact details of DPO that the affected individuals can contact for further information or assistance.

Point 9: Exceptions to Obligation to Notify Affected Individuals of a Data Breach that is Likely to have a significant harm to them

The organization may decide not to notify affected individuals (but it is still required to notify PDPC) if:

- it is able to take action which renders it unlikely that any significant harm will result to an affected individual (remedial action exception)
- there are appropriate technological measures applied to the personal data before the data breach which renders the personal data inaccessible or unintelligible to an unauthorized party (technological protection exception)
- the PDPC or law enforcement agencies may also direct the organization not to make notifications (such directions would occur where notification may compromise ongoing investigations, or where there are overriding national security or national interests)

In the event that the PDPC determines that the exception does not apply, the organization would be required to notify the affected individuals of the data breach.

Point 10: Who else to notify?

Where the organization is a receiving party to whom the personal data is disclosed, it has to notify the affected data controller about the facts of the data breach, the containment and recovery measures as well as the status, and if there are actions that the data controller needs to take to lessen the possible impact of the breach, and the DPO contact details, as soon as it is discovered without undue delay³ (no later than 24 hours) so that the affected data controller can take appropriate actions.

Where the organization is governed by a sectoral regulator, it may also need to concurrently notify the appropriate regulatory body, or according to the timeframes under their respective requirements or other written law.

Step 5: Evaluation and Response

6.14 The Data Breach Management Team will evaluate and review the cause of the breach and effectiveness of the response to it.

³As prescribed under the Personal Data Protection Act.

THE SOFTWARE PRACTICE PTE LTD	No of Pages	14 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

- 6.15 This will help reveal any systemic or ongoing problems and prevent any future breaches from occurring.
- 6.16 All breaches will be recorded regardless of whether it needs to be notified to external parties, and the outcomes and decisions made in respect of them must also be recorded.
- 6.17 The organization hopes that data breaches will be an extremely rare occurrence. However, whenever they do happen the organization understands the need to learn any lessons and tighten up security.
- 6.18 In all cases of data breach which involve human error, the staff member involved will be required to undergo refresher data protection training. Further training needs may be identified and rolled out across the organization.
- 6.19 In cases where it is a cybersecurity issue, the organization shall work to increase cybersecurity where appropriate.
- 6.20 Relevant processes and data intermediaries will be reviewed to ensure that there are no possible loopholes for a similar data breach to occur.

7 TRAINING & DEVELOPMENT

- 7.1 The organization is committed to ensuring the staff adopt the highest standards in relation to the processing and handling of personal data.
- 7.2 No member of staff will have access to any personal data unless they have been briefed on all relevant policies and practices first. Staff will be re-trained according to their needs against the tide of new guidance and legislation.
- 7.3 All existing staff will be briefed at least once every year and every time there are changes in the policies and before the changes take effect. New staff will be trained as part of employee onboarding within 1 month of their joining the organization.

8 FORMS

DPMP-PRO-03-F1	Data Breach Report
DPMP-PRO-03-F2	Data Breach Record Log
DPMP-PRO-03-F3	Data Breach Exercise Report

9 ANNEX

Annex A	Possible Data Breach Scenarios
Annex B	Drawer Plan

THE SOFTWARE PRACTICE PTE LTD	No of Pages	15 of 15
	Document Classification:	Internal
	Effective Date	10 June 2024
DATA BREACH MANAGEMENT	Doc No	DPMP-PRO-03
	Revision	1.0

ANNEX A: POSSIBLE DATA BREACH SCENARIOS

Data breaches can occur for different reasons: Possible activities (non-exhaustive) that may result in a data breach are as follows:

Malicious Activities

- Hacking, ransomware, distributed denial of service incidents or unauthorized access to databases containing personal data
- Unauthorized modification or deletion of personal data
- Theft of laptops, data storage devices or paper records containing personal data
- Scams (e.g., phishing attacks) that trick organizations into releasing personal data of individuals

Human Error

- Loss of computer notebooks, data storage devices or paper records containing personal data
- Sending personal data to a wrong e-mail or physical address, or disclosing personal data to a wrong recipient
- Unauthorized access or disclosure of personal data by employees
- Improper disposal of personal data (e.g., hard disk, storage media or paper documents)
- Poor cyber hygiene practices such as using weak or poor passwords

Computer System Weakness

- Computer hardware or software issues may also lead to data breaches. For example, errors or bugs in programming code of websites, applications and other internet downloads and usage of outdated software may be exploited to gain access to personal data stored on computer systems.

ANNEX B: DRAWER PLAN

Rev 1 / 2 May 2024

It is vital to ensure that personal data breach incident is dealt with immediately and appropriately to minimize its impact. Users should follow the Drawer Plan below for the listed scenarios.

(Note: "T" denotes the time the incident occurs)

Incident #1	Time	Task / Action	Responsibility
Staff sent email containing PD to wrong recipient	0hr (T)	1. Recall the email and immediately inform DPO upon discovering the incident. 2. Do an initial assessment to determine the details of the incident. <ul style="list-style-type: none"> • How many individuals are affected? • Are there sensitive PD such as NRIC, account details? • Send to how many wrong recipients? 3. Forward the details of the incident to the DPO.	Staff
	T + 24hrs	4. Staff to call the wrong recipient(s) to explain the details and request them to delete the email, if email recall is unsuccessful. 5. Ask the recipient(s) to give acknowledgment / confirmation that the email has been deleted. 6. Follow up with an email clearly stipulating the instruction to the recipient(s).	Staff
	T + 3 calendar days	7. If incident is likely to result in significant harm / impact to the individuals whom the personal data relates or of a significant scale (e.g., involves 500 or more individuals), report to PDPC via https://eservice.pdpc.gov.sg/case/db . <i>Notification message to PDPC to include the following:</i> <ul style="list-style-type: none"> - Facts of the data breach – summary of the facts that the organization has managed to established thus far, on a best effort basis - Approximate number of individuals and types of personal data affected by the data breach; and - If not intending to notify affected individuals, brief justification for the organization’s reliance on any applicable exception(s) - Chronology of how the organization first became aware of the data breach - Where there is a delay in the notification of the data breach to the PDPC, the reasons for the delay and the supporting evidence - Plans for managing the data breach - Whether the breach has already been rectified - Contact details of the person (DPO) whom PDPC can contact for further information or clarification 	DPO
	After notifying PDPC, not later than 24 hours	8. Unless an exception applies, notify the affected individuals of a data breach that is likely to result in significant harm or impact to them as soon as practicable, after notifying the PDPC. <i>Notification message to individual to include the following:</i> <ul style="list-style-type: none"> - Background information on how and when the data breach occurred - Types of personal data involved - Data breach management and remediation plan – what the organization has done or will be doing in response to the risks brought about by the data breach - Potential harm that the individuals might suffer from the breach - Steps that individuals might take to prevent any potential misuse of his/her personal data, or to reduce the significant harm arising from the data breach - Contact details of the DPO and how affected individuals can reach the <i>organization</i> for further information or assistance (e.g., contact numbers, email addresses) 	
	T + 5 calendar days	9. As breach occurred due to staff error, the staff will undergo a refresher personal data protection awareness training conducted by the DPO. 10. DPO to send a reminder to all employees to remind them to doublecheck the recipients before sending an email out.	DPO / Staff
The whole incident needs to be resolved within 5 calendar days.			

ANNEX B: DRAWER PLAN

Rev 1 / 2 May 2024

Incident:	Time <i>(Note: "T" denotes the time the incident occurs)</i>	Task / Action	Responsibility
Suspicious email that was clicked and led to malware into the employee computer device	0hr (T)	1. Immediately inform IT / DPO upon discovering the incident. 2. Do an initial assessment to determine the details of the incident. <ul style="list-style-type: none"> • How many individuals are affected? • Are there sensitive PD? • Is there loss of records? 	Staff DPO
	T + 1 hr	3. IT-In-Charge to do the following containment measures: <ul style="list-style-type: none"> • Do a full anti-virus scan on the device to determine any malwares • Change password on the affected device and domain password 	IT-In-Charge
	T + 24 hrs	4. IT-In-Charge to report whatever malwares or issues have been detected in their devices after the completion of the scan	DPO
	T + 24 hrs	5. Report online to SingCERT: https://www.csa.gov.sg/singcert/reporting .	DPO
After notifying PDPC, not later than 24 hours	T + 3 calendar days	6. If incident is likely to result in significant harm / impact to the individuals whom the personal data relates or of a significant scale (e.g., involves 500 or more individuals), report to PDPC via https://eservice.pdpc.gov.sg/case/db . <i>Notification message to PDPC to include the following:</i> <ul style="list-style-type: none"> - Facts of the data breach – summary of the facts that the organization has managed to established thus far, on a best effort basis - Approximate number of individuals and types of personal data affected by the data breach; and - Chronology of how the organization first became aware of the data breach - Plans for managing the data breach - Status of containment measures and other actions planned to be carried out - Contact details of the person (DPO) whom PDPC can contact for further information or clarification 	DPO
		7. Unless an exception applies, notify the affected individuals of a data breach that is likely to result in significant harm or impact to them as soon as practicable, after notifying the PDPC. <i>Notification message to individual to include the following:</i> <ul style="list-style-type: none"> - Background information on how and when the data breach occurred - Types of personal data involved - Data breach management and remediation plan – what the organization has done or will be doing in response to the risks brought about by the data breach - Potential harm that the individuals might suffer from the breach - Steps that individuals might take to prevent any potential misuse of his/her personal data, or to reduce the significant harm arising from the data breach - Contact details of the DPO and how affected individuals can reach the organization for further information or assistance (e.g., contact numbers, email addresses) 	DPO
	T + 5 calendar days	8. Conduct internal briefing to all staff on information security and remind all staff on cybersecurity threats and the do's and don't's	DPO / Staff