CONTENTS

INTRODUCTION ................................................................................................... 4

PREPARING FOR DATA BREACHES ................................................................... 6

RESPONDING TO DATA BREACHES ................................................................. 10

ANNEX A
Possible Causes of Data Breaches ................................................................. 35

ANNEX B
Data Breach Notification to the PDPC ............................................................ 36

ANNEX C
Data Breach Notification to Affected Individuals ........................................... 37
INTRODUCTION
BACKGROUND

A data breach refers to an incident exposing personal data in an organisation’s possession or under its control to the risks of unauthorised 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 organisation. 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 organisations to be accountable towards individuals by preventing and managing data breaches.

This Guide is intended to help organisations manage data breaches effectively. It also highlights key considerations for organisations in notifying the Personal Data Protection Commission (“PDPC”) and affected individuals of a data breach. This Guide is revised in view that the PDPC is intending to introduce a mandatory data breach notification requirement under the Personal Data Protection Act (“PDPA”).
PREPARING FOR DATA BREACHES
MONITORING BY ORGANISATIONS

Data breaches can occur due to various reasons, such as malicious activity, human error or computer system error (see Annex A - Possible Causes of Data Breaches for examples). It is important for organisations to put in place measures which allow them to monitor and take pre-emptive actions before data breaches occur.

Monitoring measures and tools help to provide early detection and warning to organisations. Examples include:

- Monitoring of inbound and outbound traffic for websites and databases for abnormal network activities.
- Usage of real-time intrusion detection software designed to detect unauthorised user activities, attacks and network compromises.
- Usage of security cameras for monitoring of internal and external perimeters of secure areas such as data centres and server rooms.
DATA BREACH MANAGEMENT PLAN

Planning to manage a data breach is best done early. Organisations that do not have a data breach management plan in place will find it chaotic and challenging when faced with an actual data breach. Having in place a robust data breach management plan helps organisations to manage and respond to data breaches more effectively. Such plans will need to take into account each organisation’s business processes and needs.

A data breach management plan should set out the following:

- **A clear explanation of what constitutes a data breach (both suspected and confirmed)** – This will assist employees in identifying a data breach and respond promptly should one occur.

- **How to report a data breach internally** – The role of each employee is important in reporting data breaches. When an employee becomes aware of a potential or real data breach, he or she should know how and who to report the data breach to within the organisation (e.g. specific individual(s) with expertise in handling data breaches, the data protection officer, senior management representative, data breach management team). As such, it is important to include the contact mode/details and circumstances under which that person(s) would be notified in the event of a data breach incident.

- **How to respond to a data breach** – The strategy for containing, assessing and managing data breaches would include roles and responsibilities of the employees and data breach management team. Organisations can also consider preparing contingency plans for possible data breach scenarios and measures to be taken or run regular breach simulation exercises to better prepare themselves for responding to data breaches in a prompt and effective manner. Part III of this Guide provides a general framework for responding to a data breach.
Responsibilities of the data breach management team  
– The composition and the roles and responsibilities of each member of the management team should be clear. In addition, a clear command and reporting structure of personnel at the management level who would be responsible for assessing the risks and making time-critical decisions on steps to be taken to contain and manage the data breach should be clearly established and documented. This will ensure that the organisation’s response to the data breach will not be unnecessarily delayed.
RESPONDING TO DATA BREACHES
Each data breach response needs to be tailored to the circumstances of the incident. Generally, the actions taken after a data breach should follow four key steps (using the acronym of C.A.R.E):

**STEP 1** C**ontaining the data breach to prevent further compromise of personal data.**

**STEP 2** A**ssessing the data breach by gathering the facts and evaluating the risks, including the harm to affected individuals. Where assessed to be necessary, continuing efforts should be made to prevent further harm even as the organisation proceeds to implement full remedial action.**

**STEP 3** R**eporting the data breach to the PDPC and/or affected individuals, if necessary.**

**STEP 4** E**valuating the organisation’s response to the data breach incident and consider the actions which can be taken to prevent future data breaches. Remediation efforts may continue to take place at this stage.**

The subsequent sections of this Guide will delve into the details of C.A.R.E.

In a data breach incident, it is important for organisations to ensure that their employees are aware of their roles and responsibilities (e.g. reporting, investigating, taking remedial actions) in managing the data breach.
STEP 1: CONTAIN

An organisation should act swiftly as soon as it is aware of a data breach, whether suspected or confirmed.

As mentioned above, an assigned individual or individuals should be notified of all suspected/confirmed data breaches immediately upon detection. He/she should then activate the data breach management team as the team is responsible for carrying out the actions that can reduce the potential impact of a data breach. Upon being notified, the individual members of the team should act on the information received according to their assigned role.

An initial assessment of the data breach should be conducted to determine the severity of the data breach. It will also allow the organisation to notify other stakeholders such as the internal or external legal counsel specialising in data protection and technical forensics specialists to be ready so that their expertise will be available on short notice.

The initial assessment should include (but not be limited to) the following:

- Cause of the data breach and whether the breach is still ongoing
- Number of affected individuals
- Type(s) of personal data involved
- The affected systems and/or services
- Whether help is required to contain the breach
The assessment allows organisations to decide on the immediate actions to be taken so as to contain the data breach as soon as possible. Organisations could consider the following actions, where applicable:

- Isolate the compromised system from the Internet or network, or shut down the compromised system if necessary.
- Prevent further unauthorised access to the system. Reset passwords if accounts and passwords have been compromised.
- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system.
- Stop the identified practices that led to the data breach.
- Establish whether the lost data can be recovered and steps that can be taken to minimise any harm or impact caused by the data breach (e.g. remotely disabling a lost notebook containing personal data of individuals).

The details of the data breach and post-breach response(s) should be recorded in an Incident Record Log to allow follow-up investigations or reviews. At this stage, the situation will be dynamic as more facts are unearthed while investigating the incident. Organisations should expect that as more details emerge, the initial assessment will have to be revised and the action plan reviewed.
Organisations should consider alerting the following bodies if they suspect that criminal acts have been perpetrated as these bodies may also offer assistance to the organisations in containing the data breach:

- **The Police**, if criminal activity (e.g. hacking, theft or unauthorised system access by an employee) is suspected, and to preserve evidence for investigation

- **Cyber Security Agency of Singapore** through the Singapore Computer Emergency Response Team (SingCERT) for cyber-attacks

Organisations are also advised to be mindful of the requirements set out by their respective sectoral regulators (e.g. the Monetary Authority of Singapore) for reporting of data breaches.

---

1 Cyber-attacks are deliberate exploitation of computer systems, technology-dependent enterprises and networks. It uses malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.
STEP 2: ASSESS

Upon containment of the data breach, the organisation should conduct an in-depth assessment of the data breach. Assessing the extent and likely impact of the data breach will help the organisation identify and take the appropriate steps to limit the impact of a data breach. 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 organisation in deciding whether to notify the PDPC and affected individuals.

In assessing the likely impact of the data breach, the organisation should consider the following:

**Context of the data breach**

In considering the context of a data breach, the organisation 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 disclosure of certain types of personal data, for example, national identification numbers, health records, financial information and criminal records, 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 may also be at particular risk of significant harm. For example, data breaches involving personal data that relate to minors or vulnerable individuals (e.g. victims of abuse) may exacerbate the level of harm or impact to them.

---

2 This may include physical, material or non-material harm to individuals. For example, physical safety, psychological, emotional, discrimination, identity theft or fraud, loss of business or employment opportunities, significant financial loss and damage to reputation or relationships.

3 Other contextual factors include the validity and accuracy of the personal data, and whether the data has been subjected to any form of encryption or anonymisation.
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 customer records containing full names, national identification numbers, personal mobile phone numbers and email addresses, compared to a dataset containing customers’ membership numbers and delivery addresses.

Circumstances of the data breach
The organisation 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 mentioned in page 7 may provide access, authentication, encryption, audit logs which can assist the organisation in determining how the data breach happened. The organisation should also consider if the personal data had been publicly accessible for a significant period of time before the organisation 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.
The in-depth assessment of the data breach will allow organisations to:

- conclude whether the data breach is unlikely or likely to result in significant impact or harm to the affected individuals; and

- consider, and if necessary, take 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 organisation 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. Organisations may also implement fixes to system errors/bugs to prevent further disclosure of/access to personal data.
STEP 3: REPORT

Organisations are to carry out their assessment of the data breach expeditiously within 30 days from when they first become aware of a potential data breach. Where a data breach is assessed to be likely to result in significant harm or impact to the individuals to whom the personal data relates, organisations should notify the PDPC and the affected individuals. The time frames for notifying affected individuals and the PDPC will thus commence from the time the organisation determines that the breach is eligible for reporting.

Organisations should have in place appropriate processes to notify the PDPC and the affected individuals of a data breach. In notifying the PDPC and the affected individuals, organisations should take into consideration the following points:

<table>
<thead>
<tr>
<th>Point 1</th>
<th>When do organisations need to notify the PDPC and/or affected individuals?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Organisations should notify the PDPC and/or affected individuals of a data breach that is:</td>
</tr>
<tr>
<td></td>
<td>• likely to result in significant harm or impact to the individuals to whom the information relates; or</td>
</tr>
<tr>
<td></td>
<td>• of a significant scale (i.e. data breach involves personal data of 500 or more individuals).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Point 2</th>
<th>Who do organisations need to notify?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The PDPC (by default)</td>
</tr>
<tr>
<td></td>
<td>• Affected Individuals (where appropriate, parents or guardians of young children whose personal data have been compromised), when the data breach is likely to result in significant harm or impact to the individuals to whom the information relates. This will allow the affected individuals the opportunity to take steps to protect themselves from the risks of harm or impact from the data breach (e.g. review suspicious account activities, cancel credit card, and change password).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Point 3</th>
<th>How soon do organisations need to notify?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The PDPC – as soon as practicable, no later than 72 hours after establishing that the data breach is</td>
</tr>
<tr>
<td></td>
<td>• likely to result in significant harm or impact to the individuals to whom the individual relates, or</td>
</tr>
<tr>
<td></td>
<td>• of a significant scale.</td>
</tr>
<tr>
<td></td>
<td>Affected Individuals/Others (e.g. parents of young children) – as soon as practicable.</td>
</tr>
<tr>
<td></td>
<td>Where organisations are uncertain if they should notify affected individuals, they should report to the PDPC and seek clarification.</td>
</tr>
</tbody>
</table>

4 Data breaches of a significant scale could indicate a systemic issue within the organisation, which may require the PDPC’s further investigation and guidance to the organisation on implementing the appropriate remedial actions to address it.
## Point 4
How should organisations notify the PDPC or affected individuals?

**To the PDPC:** Submit the notification at [https://eservice.pdpc.gov.sg/case/db](https://eservice.pdpc.gov.sg/case/db). For urgent notification of major cases, organisations may also contact the PDPC at +65 6377 3131 during working hours.

**To affected individuals/parents:** The PDPC will work with the organisation in deciding whether to notify the affected individuals.

Nonetheless, organisations 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. media releases, social media, e-mails, telephone calls, faxes and letters).

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

## Point 5
What details do organisations need to include in the notification?

**To the PDPC:**
- Extent of the data breach;
- Type(s) and volume of personal data involved;
- Cause or suspected cause of the breach;
- Whether the breach has been rectified;
- Measures and processes that the organisation had put in place at the time of the breach;
- Information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so; and
- Contact details of person(s) whom the PDPC could contact for further information or clarification.

**To affected individuals/parents:**
- How and when the data breach occurred;
- Types of personal data involved in the data breach;
- What the organisation has done or will be doing in response to the risks brought about by the data breach;
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
- Contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or websites); and/or
- Where applicable, what type of harm/impact the individual may suffer from the compromised data.

In both cases, where specific information of the data breach is not yet available, organisations should send an interim notification comprising a brief description of the data breach.
Notifications made by organisations or the lack of notification, as well as whether organisations have adequate recovery procedures in place, will affect the PDPC’s decision as to whether an organisation has reasonably protected the personal data in its possession or under its control.

Data intermediaries\(^5\) need not notify the PDPC or affected individuals of a data breach. Each data intermediary should instead inform its client, the organisation, of a potential or confirmed data breach without undue delay. For the purposes of this Guide, undue delay refers to a period no longer than 24 hours.

The following scenarios illustrate when organisations should consider notifying affected individuals and/or the PDPC:

**Example:**

**Theft of portable storage drive containing hotel guests’ details**

A portable storage drive containing the details of 1,000 guests of Hotel ABC was stolen. The drive included information of guests such as their full names, passport details, flight information, duration of stay with Hotel ABC, and credit card details.

As the data breach is assessed to pose a significant harm or impact to affected individuals, especially as passport and credit card details were compromised, and the scale of the data breach was significant (i.e. 500 or more affected individuals), Hotel ABC should consider notifying the PDPC and the affected individuals of the data breach.

---

\(^5\) A data intermediary is defined in section 2(1) of the PDPA as an organisation that processes personal data on behalf of another organisation but does not include an employee of that organisation.
Example:

Modification of database containing patients’ health records

The database administrator of medical clinic DEF discovered that there was an unauthorised modification of its patients’ health records. The records contained personal data of patients such as their full names, Singapore National Registration Identification Card (“NRIC”) numbers, residential addresses, medical allergies and health history. The health records of approximately 50 patients were affected.

As the data breach is assessed to pose a significant harm or impact to affected individuals, especially as NRIC numbers and health records were compromised, medical clinic DEF should consider notifying the PDPC and the affected individuals of the data breach.
Example:

**Improper disposal of client’s personal data**

An employee of voluntary welfare organisation GHI discovered that case documents containing clients’ financial, medical and family history were disposed of in an unsecured manner instead of being shredded as per the organisation’s data retention policy. However, voluntary welfare organisation GHI was not able to ascertain the scale of the data breach as the documents were sold to a ‘karang guni’ man.

As the data breach is assessed to pose a significant harm or impact to affected individuals, especially as financial and health records were compromised, voluntary welfare organisation GHI should consider notifying the PDPC of the data breach. The organisation should also assess the mode and manner of notifying the affected individuals that would best serve the interest of affected individuals when weighed against any potential anxiety and distress they may experience.
Example:

**Unauthorised access of database containing customers’ profile**

The IT administrator of online retail store JKL discovered an unauthorised access of information in its database. The database contained the personal data of 700 customers, including their full names and email addresses.

As the scale of the data breach was significant (i.e. 500 or more affected individuals), retail store JKL should consider notifying the PDPC, even though the data breach was assessed unlikely to pose significant harm or impact to the affected individuals.
Example:

**Unauthorised disclosure of students’ library loan history**

Private education institution MNO discovered an unauthorised disclosure of its students’ library loan history. The data breach involved the personal data of 250 students, including their full names, matriculation numbers and library loan history for the past one year.

As the data breach is assessed to unlikely pose a significant harm or impact to the affected individuals and is not of a significant scale, the institution may choose not to notify the PDPC nor affected students of the data breach.

However, private education institution MNO should still consider **notifying the PDPC** of the data breach if it subsequently determines that 500 or more students were affected by the data breach.
Example:

Loss of document

A member of cycling interest group PQR misplaced a document containing the cycling route of a previous cycling expedition and names of the 10 cyclists involved in the expedition.

As the data breach is assessed unlikely to pose significant harm or impact to the affected individuals and is not of a significant scale, cycling interest group PQR may choose not to notify the PDPC nor the affected cyclists.
Encryption is one of the common ways used by organisations to protect personal data. However, depending on the type of encryption used, there still lies a risk of unauthorised access of encrypted personal data, such as when thumb drives or hard disks containing encrypted data are misplaced or stolen. The following scenarios illustrates when organisations should consider notifying affected individuals and/or the PDPC:

**Example:**

**Loss of encrypted thumb drive containing insurance policy details**

A marketing director of insurance company ABC misplaced an encrypted thumb drive containing 300 policyholders’ insurance policy details such as policyholders’ names, policy numbers, names of policies and premium amounts. The encryption method used was of reasonable standards and its access was limited to only the marketing director. The insurance company assessed that third party access to the encrypted data of the misplaced thumb drive was unlikely.

Given that the personal data was encrypted in the thumb drive to prevent unauthorised access, the misplaced thumb drive was assessed unlikely to pose significant harm or impact to the affected individuals. In addition, the encrypted data did not reach the significant scale of 500 or more individuals. As such, insurance company ABC may choose not to notify the PDPC or the affected customers.
Example:

Loss of laptop containing health information

Pharmaceutical research laboratory STU maintains a list of patients with a rare communicable disease. The list contains personal data of 1,000 patients, including their full names, medical history and treatment details. Only researchers who deal with these patients are given access to the list. The list is stored in the pharmaceutical research laboratory’s intranet and can also be accessed with the correct credentials through authorised laptops. There are three layers of security measures put in place for accessing these laptops - (i) BIOS password; (ii) bitlocker; and (iii) Windows password. One of their researchers loses his authorised laptop.

Pharmaceutical research laboratory STU assessed that it was unlikely that a third party could overcome the three layers of protection measures put in place for access to the laptop. In addition, the credentials of the researcher were not stored on the laptop. Hence, the lost laptop did not pose a risk of significant harm or impact to the affected patients. However, as the number of potentially affected individuals was 500 or more, the pharmaceutical research laboratory proceeded to notify the PDPC of the data breach. The reporting will allow the PDPC to assess whether there is any inherent problem within the organisation if, for example, there is an increasing trend of similar incidents occurring within a short period of time. The PDPC may provide some advice to the organisation on taking preventive measures to lower the risk of occurrence of similar incidents.
**STEP 4: EVALUATE**

Where the containment efforts/initial remedial actions were ineffective and more lapses are found, the organisation may also implement other remedial actions to further reduce the harm to the affected individuals.

In addition, the organisation should review and learn from the data breach incident to improve its personal data handling practices and prevent the reoccurrence of similar data breaches. In doing so, the organisation may consider the following areas:

<table>
<thead>
<tr>
<th>OPERATIONAL- AND POLICY-RELATED ISSUES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data breach management plan and response</strong></td>
</tr>
<tr>
<td>• Was the data breach management plan <strong>effective</strong> in responding to the data breach incident? Were there any areas where the plan could be improved?</td>
</tr>
<tr>
<td>• Were data breach response plans <strong>tested regularly</strong> to ensure effectiveness?</td>
</tr>
<tr>
<td>• Is there a need to develop <strong>new</strong> data breach scenarios?</td>
</tr>
<tr>
<td>• Was there a <strong>clear line of responsibility and communication</strong> during the management of the data breach?</td>
</tr>
<tr>
<td>• Were pre-defined modes of communication <strong>effective</strong> during the data breach incident response?</td>
</tr>
<tr>
<td><strong>Existing measures and processes</strong></td>
</tr>
<tr>
<td>• Were <strong>audits</strong> regularly conducted on both physical and IT-related security measures? Were the action items from the audits remediated?</td>
</tr>
<tr>
<td>• Are there <strong>processes</strong> that can be streamlined or introduced to limit the damage if future data breaches happen or to prevent a relapse?</td>
</tr>
<tr>
<td>• Were there <strong>weaknesses in existing security measures</strong> (e.g. use of outdated software and protection measures such as weak passwords)?</td>
</tr>
<tr>
<td>• Were there <strong>weaknesses in the use of portable storage devices or connectivity to the Internet</strong>?</td>
</tr>
<tr>
<td>• Were the methods for <strong>accessing and transmitting personal data</strong> sufficiently secure (e.g. access only limited to authorised personnel)?</td>
</tr>
<tr>
<td><strong>Roles of external parties</strong></td>
</tr>
<tr>
<td>• Should <strong>support services</strong> from external parties, such as vendors and partners, be enhanced, to better protect personal data?</td>
</tr>
<tr>
<td>• Were the <strong>responsibilities</strong> of vendors and partners clearly defined in relation to the handling of personal data?</td>
</tr>
</tbody>
</table>
### MANAGEMENT-RELATED ISSUES

<table>
<thead>
<tr>
<th>Managing the data breach</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• How was senior management involved in the management of the data breach?</td>
<td></td>
</tr>
<tr>
<td>• Was there sufficient or effective direction given in managing the data breach?</td>
<td></td>
</tr>
</tbody>
</table>

### EMPLOYEE- & RESOURCE-RELATED ISSUES

<table>
<thead>
<tr>
<th>Training</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Were employees aware of security related issues?</td>
<td></td>
</tr>
<tr>
<td>• Was training provided on personal data protection matters and incident management skills?</td>
<td></td>
</tr>
<tr>
<td>• Were employees informed of the data breach and the learning points from the incident?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Responding to the data breach</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Was there an appointment of a competent and qualified data breach incident response manager/team?</td>
<td></td>
</tr>
<tr>
<td>• Did the manager/team understand and properly execute the data breach management plan?</td>
<td></td>
</tr>
<tr>
<td>• Were there enough resources to manage the data breach?</td>
<td></td>
</tr>
<tr>
<td>• Should external resources be engaged to better manage such incidents?</td>
<td></td>
</tr>
<tr>
<td>• Were key personnel given sufficient resources to manage the incident?</td>
<td></td>
</tr>
</tbody>
</table>
Summary of the data breach response process:

Staff should report all suspected/confirmed data breaches to a specific individual or individuals, with expertise in handling personal data and data breaches immediately.

Data breach management team should conduct an initial assessment of the data breach to assess the severity. This should include the following:

- Cause of the data breach and whether the breach is still ongoing
- Number of individuals affected
- Types of personal data disclosed
- Systems and/or services affected
- Whether help is required to contain the breach

Act swiftly to contain the breach (i.e. taking immediate steps to limit any further access to or disclosure of the personal data).

Record the data breach and the organisation’s response(s) in an Incident Record Log.

Data Intermediaries should report data breaches to the main organisation without undue delay (no later than 24 hours) from the time it first becomes aware of the breach.
An in-depth assessment of the data breach can help an organisation understand the risks posed by the data breach and how these risks can be addressed.

When assessing the breach, consider the following:
- The circumstances of the data breach, including its cause and extent
- The types of personal data involved
- The number and groups of affected individuals
- Risks involved
- Whether external help is required
- Remedial actions which can be taken if deemed necessary

When evaluating risks posed by the data breach, consider the following:
- Sensitivity of the data involved
- Presence of mitigating factors (e.g. encryption)
- What happened to the data
- The nature of harm to the affected individuals (if any)

Through the assessment, organisations should be able to conclude whether the data breach was unlikely or likely to result in causing significant harm to the affected individuals.
Organisations should notify the PDPC as soon as practicable, no later than 72 hours from the time the organisation has made its assessment.

Organisations may send an email to notify the PDPC of the data breach.

Refer to Annex B for more details.

Organisations should also notify affected individuals as soon as practicable. Notifications should include (but not be limited to) the following:

- Specific facts on the data breach
- Actions individuals can take
- Organisation’s contact details

Refer to Annex C for more details.
Review and take action to prevent future breaches. This may include the following:

- Implementation/continuing efforts of the remediation actions
- Identification of areas of weakness and taking action to strengthen them
- Effectiveness of the organisation’s data breach response(s)
- Corrective actions to be taken
CONCLUDING REMARKS

Having in place a data breach management plan is important as it will enable organisations to respond swiftly in managing any data breaches in a systematic manner. Organisations are encouraged to proactively develop and implement a robust data breach management and response plan, and to review the plan regularly to ensure it remains effective and relevant as business operations evolve.

For more information on the PDPA, or to view our other guides and advisory guidelines, please visit [www.pdpc.gov.sg](http://www.pdpc.gov.sg).
ANNEX A

POSSIBLE CAUSES OF DATA BREACHES

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

**Malicious activities**

Malicious activities could be perpetrated by an external party or from within the organisation, such as:

- Hacking incidents/Illegal access to databases containing personal data
- Theft of computer notebooks, data storage devices or paper records containing personal data
- Scams that trick organisations into releasing personal data of individuals

**Human error**

Typically, human errors could be caused by employees, such as:

- 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 data to a wrong recipient
- Unauthorised access or disclosure of personal data by employees
- Improper disposal of personal data (e.g. hard disk, storage media or paper documents containing personal data sold or discarded before data is properly deleted)

**Computer system error**

Computer hardware or software issues may also lead to data breaches, e.g. errors or bugs in the programming code of websites, databases and other software which may be exploited to gain access to personal data stored on computer systems.
ANNEX B

DATA BREACH NOTIFICATION TO THE PDPC

Inform the PDPC by submitting a notification at https://eservice.pdpc.gov.sg/case/db. For urgent notification of major cases, organisations may also contact the PDPC at +65 6377 3131 during work hours.

The notification should include the following information, as far as possible:

• Extent of the data breach;
• Type(s) and volume of personal data involved;
• Cause or suspected cause of the breach;
• Whether the breach has been rectified;
• Measures and processes that the organisation had put in place at the time of the breach;
• Information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so: and
• Contact details of person(s) whom the PDPC could contact for further information or clarification.

Where specific information of the data breach is not yet available, organisations should send an interim notification comprising a brief description of the incident.

Notifications made by organisations or the lack of notification, as well as whether organisations have adequate recovery procedures in place, will affect the PDPC’s decision on whether an organisation has reasonably protected the personal data in its possession or under its control.
ANNEX C

DATA BREACH NOTIFICATION TO AFFECTED INDIVIDUALS

Organisations should assess which is the most effective way to notify affected individuals of the data breach. The notification should include the following information, where available:

- How and when the data breach occurred;
- Types of personal data involved in the data breach;
- What the organisation has done or will be doing in response to the risks brought about by the data breach;
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
- Contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or websites); and/or
- Where applicable, what type of harm/impact the individual may suffer from the compromised data.

Where specific information of the data breach is not yet available, organisations should send an interim notification comprising a brief description of the incident.

---

6 The PDPC recognises that there are many different modes of notification that could evolve with technology, and organisations should be allowed to determine the most efficient and expedient mode of notification to inform affected individuals as soon as practicable so that they may take actions to mitigate the potential risk of harm or loss from the breach.
Singapore Digital (SG:D) gives Singapore's digitalisation efforts a face, identifying our digital programmes and initiatives with one set of visuals, and speaking to our local and international audiences in the same language.

The SG:D logo is made up of rounded fonts that evolve from the expressive dot that is red. SG stands for Singapore and :D refers to our digital economy. The :D smiley face icon also signifies the optimism of Singaporeans moving into a digital economy. As we progress into the digital economy, it's all about the people - empathy and assurance will be at the heart of all that we do.