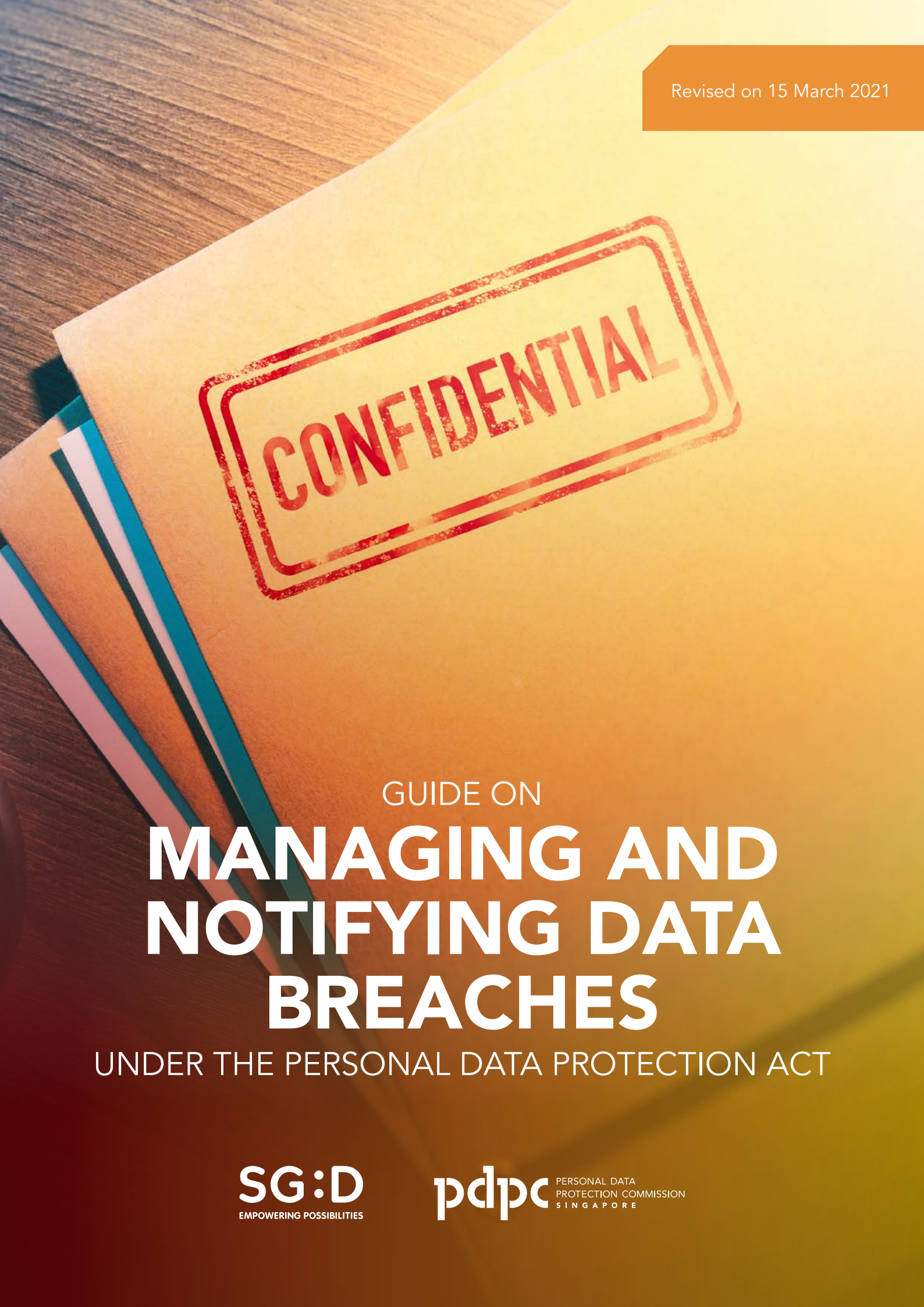


Revised on 15 March 2021

GUIDE ON

MANAGING AND NOTIFYING DATA BREACHES

UNDER THE PERSONAL DATA PROTECTION ACT

SG:D
EMPOWERING POSSIBILITIES

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CONTENTS

EXECUTIVE SUMMARY

DEMONSTRATING ACCOUNTABILITY BY PREVENTING, MANAGING AND REPORTING DATA BREACHES

Data breaches can 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**") can be exposed to significant harm if they do not take steps to protect themselves. Hence it is important for organisations to be accountable towards individuals by preventing, managing and notifying the Personal Data Protection Commission ("**PDPC**" or the "**Commission**") and affected individuals of data breaches.

Part I of the Guide recommends good practices that help organisations to identify and prepare for data breaches with a data breach management plan. Part II sets out key considerations for organisations in responding to data breaches. The suggested actions taken in the event of a data breach should follow four key steps (using the acronym of **C.A.R.E**):

- **Contain** the data breach to prevent further compromise of data and implement mitigating action(s) to minimise potential harms from the breach after an initial appraisal has been conducted to determine the extent of the breach.
- **Assess** the data breach to determine the root cause (where possible) and the effectiveness of containment action(s) taken thus far to contain the data breach. Where necessary, continuing efforts should be made to prevent further harm from the data breach.
- **Report** the data breach to:
  - The PDPC (mandatory if the breach is a notifiable data breach under the Personal Data Protection Act ("**PDPA**"). Organisations may also inform PDPC of the data breach voluntarily); and/or
  - The affected individuals (if required under the Data Breach Notification Obligation ("**DBN Obligation**")).
- **Evaluate** the organisation's response to the data breach and consider the actions that can be taken to prevent future data breaches. Where necessary, continuing efforts should be made to prevent further harm from the data breach.

Part III of the Guide provides an outline of the mandatory DBN Obligation, including the criterion, timelines and information to be provided when notifying the PDPC and affected individuals. For more information on the DBN Obligation, organisations may refer to the following resources:

- DBN Obligation section of the Advisory Guidelines on Key Concepts in the PDPA
- Personal Data Protection (Notification of Data Breaches) Regulations 2021

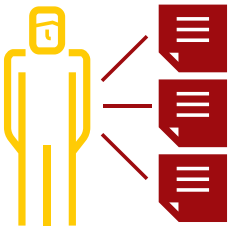
The Guide focuses on managing the data breach incidents and does not exhaustively address every scenario nor specify the processes or systems that organisations should put in place to prevent future occurrence. Each data breach response needs to be tailored to the circumstances of the incident. Organisations are encouraged to consider how the suggestions within the Guide may be applied to their specific circumstances and to seek professional advice where required. Organisations should also consider whether additional measures are required to address the root cause(s) of the data breach.

PART I: PREPARING FOR DATA BREACHES

DEFINING AND MONITORING FOR DATA BREACHES

A data breach, in relation to personal data, refers to any unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data. It also includes the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

A data breach can be the result of malicious activities, human error or computer system weaknesses. Annex A provides more examples of possible causes of data breaches.



MONITORING BY ORGANISATIONS

As data breaches can occur for different reasons, it is important for organisations to put in place measures which allow them to monitor and take pre-emptive actions to prepare for data breaches. Organisations may take a risk-based approach in identifying risks of data breaches and designing monitoring methods and effective remediation measures.

Monitoring should be done by both regular management oversight and using of monitoring tools. Logs from operating systems, applications and network devices should be regularly reviewed for anomalies and can help to identify malicious attacks on systems. Organisations may also subscribe to information sources such as SingCERT alerts and advisories on security issues, vulnerabilities and exploits which provide information on the latest security trends. Such information increases organisations' awareness of possible risks and threats they may be exposed to when using products and services, allowing them to take action to mitigate the risks and vulnerabilities as soon as possible.

Monitoring tools help to provide early detection and warning to organisations. The usage of automated tools where possible can increase effectiveness and efficiency during monitoring and incident response. Examples include:

- Monitoring of inbound and outbound traffic for abnormal network activities of websites and databases.
- 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

Having in place a data breach management plan is important as it will enable organisations to respond swiftly by 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.

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.

Response time is a key factor in minimising impact from data beaches. As such,organisations should keep employees and key stakeholders updated of its data breach management plans to contain and mitigate the impact of data breaches quickly and effectively. Periodic exercises or walkthroughs should also be conducted so that key actors in the data breach management plans are familiar with their roles.

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 to respond promptly should one occur.

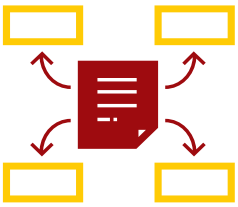
Steps to report a data breach internally — The role of each employee is important in reporting data breaches. When an employee becomes aware of a potential or real data breach, he or she should know how and who to report the data breach to within the organisation (e.g., specific individual(s) with expertise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

Apart from data breach management plans, organisations may also consider developing crisis management, communications and business continuity plans to aid in their handling of data breaches and recovery from such incidents.

PART II: RESPONDING TO DATA BREACHES



CONTAIN, ASSESS, REPORT, EVALUATE (C.A.R.E)

Each data breach response needs to be tailored to the circumstances of the incident. Generally, the actions taken in the event of a data breach should follow four key steps (using the acronym of C.A.R.E):

C **ontain** the data breach to prevent further compromise of data and implement mitigating action(s) to minimise potential harms from the breach.

A **ssess** the data breach by gathering the facts and assessing the effectiveness of containment action(s) taken thus far before proceeding to implement full remedial actions. Where necessary, continuing efforts should be made to prevent further harm from the data breach.

R **eport** the data breach to:

- The PDPC (mandatory if the breach is a notifiable data breach under the PDPA. Organisations may inform PDPC of the breach voluntarily); and/or
- The affected individuals (if required under the DBN Obligation).

E **valuate** response to the data breach and consider the actions which can be taken to prevent future data breaches.

CONTAIN

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

An assigned individual or group should be immediately notified of all suspected/confirmed data breaches 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 activation, the members of the team should act on the information received according to their assigned role.

An initial appraisal 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 appraisal of the breach should include (but not be limited to) the following considerations. The information from this stage may also be relevant to organisations' DBN Obligation, which is discussed in the following section:

- 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, servers, databases, platforms, services etc.
- Whether help is required to contain the breach
- The remediation action(s) that the organisation has taken or needs to take to reduce any harm to affected individuals resulting from the breach

Having the above information will help organisations to decide on the immediate actions to be taken so as to contain the data breach as soon as possible. Organisations can consider the following immediate containment actions, where applicable:

- Isolate the compromised system from the Internet or network by disconnecting all affected systems
- Re-route or filter network traffic, firewall filtering, closing particular ports or mail servers
- Prevent further unauthorised 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 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 implement further action to minimise any harm caused by the data breach (e.g., remotely disabling a lost notebook containing personal data of individuals, recalling an email that has been accidentally sent or forwarded etc.)

The details of the data breach (such as summary of the incident and chain of events) and post-breach response(s) should be recorded in an Incident Record Log. Organisations may also wish to obtain forensic copies and logs of the affected IT systems for follow-up investigations, incident resolution and legal proceedings purposes. 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 updated 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 (CSA)** through the Singapore Computer Emergency Response Team (SingCERT) for cyber incidents[1].

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

ASSESS

Upon containment of the data breach, the organisation must conduct an in-depth assessment of the data breach, the success of its containment action(s) taken, or the efficacy of any technological protection (e.g., effectiveness of any encryption) applied on the personal data involved in the breach. Where necessary, organisations should continue their efforts to reduce potential harm to the affected individuals.

Understanding the extent and likely impact of the data breach will help the organisation identify and take further steps to limit the harm[2] resulting from a data breach and prevent the recurrence of similar incidents. Crucially, the organisation will also have to determine if it is required to notify the PDPC and/or affected individuals of the breach under the DBN Obligation. Section on Criteria for Data Breach Notification in Part III of the Guide provides key information on the criteria for the mandatory DBN Obligation.

[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.

[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.

Once an organisation has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), the organisation must take reasonable and expeditious steps to assess whether the data breach is notifiable under the PDPA, and document the steps taken in assessing the data breach. Any unreasonable delay in assessing a data breach will be a breach of the DBN Obligation, allowing the PDPC to take enforcement action.

In general, organisations must assess if the data breach is a notifiable one. If an organisation is unable to complete its assessment within 30 days, the organisation should be prepared to provide the PDPC with an explanation for the time taken/required to carry out the assessment.

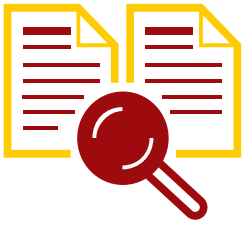
The following considerations would help organisations in their assessment of the data breach:

- **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 (e.g., minors, vulnerable individuals etc.), and other contextual factors such as whether the personal data was publicly available before the data breach[3].

- **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 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, age, and personal mobile phone numbers, compared to a dataset containing customers' membership numbers and delivery addresses.

[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.

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 monitoring tools mentioned in Part I of the Guide may also help the organisation determine how the data breach occurred. The organisation should also consider if the compromised personal data had been made publicly accessible for a significant period of time before the organisation became aware of the data breach. The likelihood that the personal data had been accessed and used in ways that could result in harm increases with the duration of time it had been exposed.



REPORT

Depending on the outcome of assessment, the data breach may have to be notified to the PDPA and affected individuals. Section on Timeframes for Notification in Part III of the Guide provides key information on the mandatory DBN Obligation, including the timelines and information to be provided when notifying the PDPC and affected individuals.

Organisations may choose to voluntarily notify the PDPC even if they assess that the data breach is not a mandatorily notifiable one under the PDPA. This depends on the organisation's internal risk assessment, policies and procedures. Notification also allows the PDPC to assess the circumstances and impact of the data breach and provide timely guidance on the appropriateness of the remedial actions taken by the organisations. Voluntary notifications send a message that an organisation is committed to be accountable for protecting data, and has systems and processes in place to mitigate risks should data breaches occur. As such, the PDPC may consider voluntary notifications as a mitigating factor when considering the appropriate enforcement actions to undertake.

Effective notification to affected individuals provides them with the opportunity to take steps to protect their personal data following a data breach, such as changing their account passwords or being alert to possible scams resulting from the breach. It also helps to build consumer trust in the organisation as it demonstrates that the organisation is accountable and makes data protection a priority.

Section 26D(2) of the PDPA prescribes that organisations must notify affected individuals as soon as practicable, at the same time or after notifying the Commission. However, for data breaches which are likely to attract widespread public attention and/or interest, or those which organisations require guidance on notifying the affected individuals, organisations are **strongly encouraged** to notify and seek advice from the PDPC first before notifying the affected individuals.

EVALUATE

Organisations should review and learn from the data breach to improve its personal data handling practices and prevent the recurrence of similar data breaches. This may involve:

- A review including a root cause analysis of the data breach (e.g., implement fixes to system errors/bugs to prevent future disclosure of/access to personal data)
- A prevention plan to prevent similar data breaches in future
- Audits to ensure the prevention plan is implemented
- A review of existing policies, procedures and changes to reflect the lessons learnt from the review
- Changes to employee selection and training practices
- A review of data intermediaries involved in the data breach

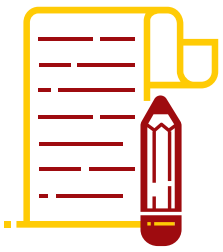
Annex B provides further information on areas that an organisation may consider in its post-breach evaluation.

Annex C is a cyber incident response checklist. Organisations may also use the checklist when developing their incident response and data breach management plans.

PART III: THE DATA BREACH NOTIFICATION OBLIGATION

This section sets out key information on the DBN Obligation. For more information, organisations should refer to the following resources:

- DBN Obligation section of the Advisory Guidelines on Key Concepts in the PDPA
- Personal Data Protection (Notification of Data Breaches) Regulations 2021("**PDP (DBN) Regulations 2021**")



REQUIREMENTS FOR ORGANISATIONS AND DATA INTERMEDIARIES

Part 6A of the PDPA sets out the requirements for organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or the Commission where it is assessed to be notifiable. Data intermediaries that process the personal data on behalf and for the purposes of another organisation (including a public agency) are also required to notify that other organisation or public agency of a data breach detected.

DUTY TO CONDUCT ASSESSMENT OF DATA BREACH

Once an organisation has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), the organisation is required to take reasonable and expeditious steps to assess whether the data breach is notifiable under the PDPA within 30 calendar days. Any unreasonable delay in assessing a data breach will be a breach of the DBN Obligation and the Commission can take enforcement action. If an organisation is unable to complete its assessment within 30 days, it would be prudent for the organisation to be prepared to provide the Commission with an explanation for the time taken/ required to carry out the assessment.

To demonstrate that it has taken reasonable and expeditious steps to assess whether the data breach is notifiable, the organisation must document all steps taken in assessing the data breach[4].

[4] The organisation may be required to produce supporting documentation on the steps taken for its assessment of the data breach as part of its notification to the Commission, or for any investigation by the Commission of a suspected breach.

CRITERIA FOR DATA BREACH NOTIFICATION

Significant Harm to Affected Individuals

Organisations are required to assess whether a data breach is notifiable as it is likely to result in significant harm[5] to the affected individuals. Given the likelihood of harm arising from a data breach, notification ensures affected individuals are aware and able to take steps to protect themselves (e.g., change password, cancel credit card, monitor account for unusual activities).

To provide certainty to organisations on the data breaches that are notifiable, the PDP (DBN) Regulations 2021 provides the personal data (or classes of 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 organisation will be required to notify the affected individuals and the Commission of the data breach.

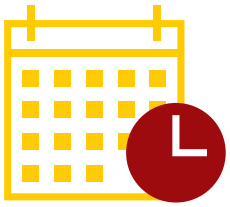
[5] Significant harm could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation and other forms of harms that a reasonable person would identify as a possible outcome of a data breach.

Significant Scale

Data breaches of a significant scale may indicate a systemic issue within the organisation. Notifying the Commission of such data breaches will allow it to provide guidance to organisations on remedial actions to address the data breach as well as any systemic changes to prevent future occurrences.

Data breaches that meet the criteria of significant scale are those that involve the personal data of 500 or more individuals. Where a data breach affects 500 or more individuals, the organisation is required to notify the Commission, even if the data breach does not involve any prescribed personal data in the PDP (DBN) Regulations 2021.

If an organisation is unable to determine the actual number of affected individuals in a data breach, the organisation should notify the Commission when it has reason to believe that the number of affected individuals is at least 500. This may be based on the estimated number from an initial appraisal of the data breach. The organisation may subsequently update the Commission of the actual number of affected individuals when it is established.



TIMEFRAMES FOR NOTIFICATION

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

a. the Commission as soon as practicable, but in any case, no later than three (3) calendar days[6]; and

b. where required, affected individuals as soon as practicable, at the same time or after notifying the Commission.

These timeframes for notifying the Commission and/or the affected individuals commences from the time the organisation determines that the data breach is notifiable. Any unreasonable delays in notifying the relevant parties will be a breach of the DBN Obligation.

Where an organisation is required to notify affected individuals of a data breach, it should notify the affected individuals at the same time or after it notifies the Commission.

Annex D provides an infographic on the timelines for assessment and notification of data breaches to the PDPC and affected individuals.

INFORMATION TO BE PROVIDED IN NOTIFICATION OF A DATA BREACH

An organisation notifying affected individuals and/or the Commission of a notifiable data breach is required to provide relevant details of the data breach to the best of its knowledge and belief. The notification should also include relevant information about the organisation's data breach management and remediation plans (covered in Part I of the Guide). Please refer to the PDP(DBN) Regulations 2021 for more information.

[6] The first day of the three days starts on the day after the organisation makes the determination that there is a notifiable breach. To illustrate, if an organisation determines on 1st January that a data breach is notifiable, it must notify the Commission by 4th January.

NOTIFICATION TO THE COMMISSION

Submit the 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 working hours.

To ensure proactive steps are taken by the organisation to manage and remediate the data breach, information to be provided in the organisation's notification to the Commission shall include:

a. Facts of the data breach

i. The date on which and the circumstances in which the organisation first became aware that a data breach has occurred;

ii. Information on how the notifiable data breach occurred;

iii. The number of affected individuals affected by the notifiable data breach;

iv. The personal data or classes of personal data affected by the notifiable data breach; and

v. The potential harm to the affected individuals as a result of the notifiable data breach.

b. Data breach handling

i. A chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment under section 26C(2) or (3)(b) of the PDPA that the data breach is a notifiable data breach;

ii. Information on any action by the organisation, whether taken before or to be taken after the organisation notifies the Commission of the occurrence of the notifiable data breach –

a. To eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and

b. To address or remedy any failure or shortcoming that the organisation believes to have caused, or have enabled or facilitated the occurrence of, the notifiable data breach; and

iii. Information on the organisation's plan (if any) to inform all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach. The organisation may provide in general terms the steps taken or intended to be taken.

c. Contact details

i. Contact details of at least one authorised representative of the organisation. The representative(s) need not be the organisation's DPO (or a person assuming the DPO's responsibilities in the organisation).

Where the data breach notification to the Commission is not made within three (3) calendar days of ascertaining that it is a notifiable breach, the organisation must also specify the reasons for the late notification and include any supporting evidence. The reasons for the late notification will go toward the gravity of the organisation's contravention of the DBN Obligation and consequently the nature and severity of the penalties imposed on the organisation, if any.

Where the organisation does not intend to notify any affected individual, the notification to the Commission must additionally specify the grounds (whether under the PDPA or other written law[7]) for not notifying the affected individual.

[7] For instance, in reliance on any application exceptions in section 26D(5) or (6)(a) of the PDPA, or any prohibition or restriction under other written law.

NOTIFICATION TO AFFECTED INDIVIDUALS

Notification to affected individuals should be clear and easily understood. It should include guidance on the steps affected individuals may take to protect themselves from the potential harm arising from the data breach. Where appropriate, organisations should notify parents or guardians of young children whose personal data has been compromised.

Where the data breach involves information related to adoption matters or the identification of vulnerable individuals, organisations should first notify the Commission for guidance on notifying affected individuals.

Organisations are not required to provide to the Commission the notification to be sent to affected individuals. Organisations should include the following information in their notifications to affected individuals:

a. Facts of the data breach

i. The circumstances in which the organisation first became aware that a notifiable data breach has occurred; and

ii. The personal data or classes of personal data relating to the affected individual affected by the notifiable data breach.

b. Data breach management and remediation plan

i. Potential harm to the affected individual as a result of the notifiable data breach;

ii. Information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual –

a. To eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach;

b. To address or remedy any failure or shortcoming that the organisation believes to have caused, or have enabled or facilitated the occurrence of, the notifiable data breach; and

iii. Steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the affected individual's personal data affected by the notifiable data breach.

c. Contact details

i. Contact details of at least one authorised representative whom the affected individual can contact for further information or assistance. The representative(s) need not be the organisation's DPO (or a person assuming the DPO's responsibilities in the organisation), or the same representative provided in the organisation's notification to the Commission.

Organisations may customise their notification to affected individuals, as long as it includes the required content. In addition, decision on the appropriate actions that the individual may take is dependent on the circumstances of the data breach. This may include choosing to tailor the recommended protective actions that individuals could take depending on the individual's circumstances or providing general recommendations that apply to all affected individuals.

NOTIFICATION TO OTHER REGULATORS

Where an organisation is required to notify a sectoral regulator or law enforcement agency of a data breach under other written laws, the organisation must notify that sectoral regulator or law enforcement agency accordingly. Additionally, it must also notify the PDPC and/or affected individuals (if required) according to the timeframes for data breach notification under the PDPA. An organisation is not regarded to have fulfilled the DBN Obligation under the PDPA just by fulfilling any other breach notification requirements set out under other written laws.

ANNEX A

POSSIBLE CAUSES OF DATA BREACHES

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

Malicious Activities

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

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

Human Error

Typically, human errors can 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 personal 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)
- Poor cyber hygiene practices such as using of weak or poor passwords

Computer System Weaknesses

Computer hardware or software issues may also lead to data breaches. For example, errors or bugs in the programming code of websites, databases, 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

POST-BREACH EVALUATION

ROOT CAUSE ANALYSIS AND POST-BREACH ACTIONS TAKEN	
Root cause analysis	• What was the chronological timeline of events that led up to the incident? • What weakness did the breach exploit, e.g., systems, procedures, people? Was this a new issue or an issue that we had already knew about? • Were there existing procedures that could have addressed the breach and were the processes followed? • Were there signs that were missed? Does monitoring need to be refined? • What were the probable causes and the underlying cause that led to the breach?
Post-breach actions taken	• What had been done to contain the breach short term? • What had been done to contain the breach long-term to prevent a similar incident from happening? • Were there backups of the affected systems to help restore operations? • How long will the affected systems be monitored and what to look for when monitoring?

ANNEX B

POST-BREACH EVALUATION

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

ANNEX B

POST-BREACH EVALUATION

MANAGEMENT-RELATED ISSUES	
Managing the data breach	• How was senior management involved in the management of the data breach? • Was there sufficient or effective direction given in managing the data breach?

EMPLOYEE AND RESOURCE-RELATED ISSUES	
Training	• Were employees aware of security-related issues? • Was training provided on personal data protection matters and incident management skills? • Were employees informed of the data breach and the learning points from the incident?
Responding to the data breach	• Was there an appointment of a competent and qualified data breach incident response manager/team? • Did the manager/team understand and properly execute the data breach management plan? • Were there enough resources to manage the data breach? • Should external resources be engaged to better manage such incidents? • Were key personnel given sufficient resources to manage the incident?

ANNEX C

CYBER INCIDENT RESPONSE CHECKLIST

This checklist is jointly developed by the Cyber Security Agency of Singapore and the Personal Data Protection Commission. It is meant to guide organisations in stressful and high-pressured situations to contain and recover from an incident quickly and effectively. Following the four key steps (using the acronym C.A.R.E.), the checklist can improve response time and minimise damages.

CONTAIN

Following the discovery of the incident, the designated incident response team should be notified immediately to ensure that the incident is dealt with swiftly and efficiently.

Alerting relevant parties of the incident	**Incident response team:** □ Incident response handler □ Incident response service provider □ Product/service vendor(s) **Organisations may consider alerting the following bodies:** □ Regulatory bodies □ Law enforcement agencies □ SingCERT □ Business clients (if you are a service provider, e.g., data intermediary) □ Others: _____
Knowing your IT infrastructure	**Identify investigation resources:** □ List of key assets and data and where they are located/hosted □ Network diagrams □ Current baseline of IT systems' activities □ Documentation of IT systems and software versions □ Backing-up of important data □ Others: _____

Recognising possible attack vectors	**Organisations should identify common attack vectors or entry points that threat actors may use, such as:** □ Poorly designed web applications □ Misconfigured systems □ Internet downloads □ Poor cyber hygiene practices (e.g., use of weak or default passwords, use of outdated software, etc.) □ Human lapses □ Authorised third parties □ Others: _____
Reviewing possible sources of precursors and indicators	□ Security software (e.g., Intrusion Detection Systems [IDS], Security Information and Events Management System [SIEM], anti-virus software, third party monitoring services etc.) □ Logs (e.g., operating system logs, service and application logs, network device logs, netflow logs etc.) □ Publicly available information (e.g., SingCERT alerts & advisories, alerts & advisories from products/services vendors on vulnerabilities etc.) □ People from within your organisation □ Others: _____
Making an initial assessment and prioritising the next steps	□ Correlate events against the baseline to determine if an incident has occurred □ Check incidents against known threat precursors and indicators □ Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch □ Prioritise the incident handling activities, including whether to activate crisis management, and crisis communications plans □ Others: _____
Developing Containment Strategies	Containment strategies vary depending on the type of incident, and a strategy should be developed for different incident types to contain the incident and minimise the damage. Some of the more common strategies are: □ Isolate all or parts of the compromised network by disconnecting all affected systems □ Re-route or filter network traffic □ Firewall filtering □ Closing particular ports or mail servers □ Block further unauthorised access to the system □ Others: _____

ASSESS

Following identification and containment of the cyber incident, organisations may conduct an in-depth assessment of the incident to understand its impact and severity. The information gathered during this phase allows the organisation to decide whether further remedial actions are required and devise strategies for recovery. The threats/vulnerabilities have to be thoroughly eradicated before normal operations can resume to minimise subsequent repeated disruptions.

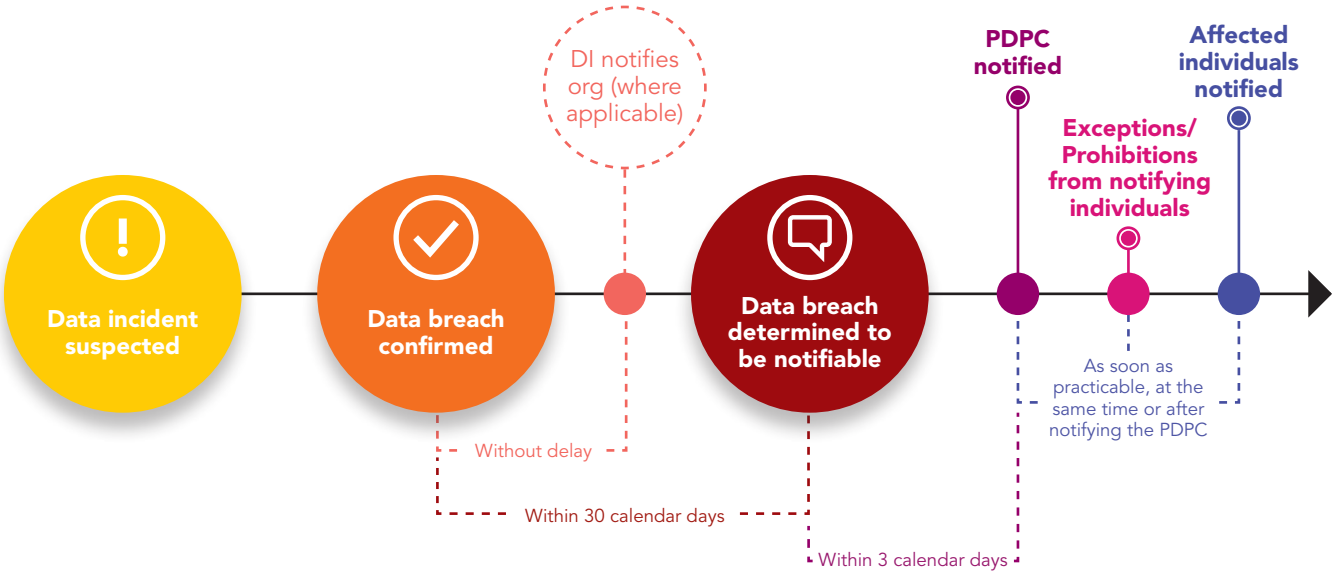
Gathering evidence	Evidence gathering may serve two purposes – incident resolution and legal proceedings. Some of the evidence that need to be documented and/or preserved include: □ Summary of the incident □ Incident indicators □ System events □ Actions taken during the incident □ Logs of affected systems □ Forensic copies of affected systems □ Others: _____
Eradicating the threat	After containing the incident, eradication may be necessary to eliminate all traces of the incident. This may include: □ Wiping out the malware □ Disabling breached user accounts □ Patching vulnerabilities that were exploited. This should be applied to all affected hosts within the organisation □ Others: _____
Taking steps towards recovery	This may entail: □ Restoring systems from backups □ Rebuilding systems from scratch □ Installing patches □ Changing passwords (both administrators and users) □ Tightening network perimeter security □ Confirming the integrity of business systems and controls □ Others: _____

REPORT	
Knowing your Stakeholders and/or Fiduciary Obligations	Notify relevant stakeholders and affected parties: □ Board of Directors □ Regulators, law enforcement and other government agencies (e.g., SPF, PDPC, CSA, SGX etc.) □ Clients □ Media □ Others: _____

EVALUATE Organisations should proactively review their incident response plans and activities to identify and resolve deficiencies, and strengthen their security posture. They should also engage in continuous monitoring of their networks for abnormal activities and make sure that threat actors have been inhibited thoroughly.	
Monitoring and maintaining vigilance	□ Continue to monitor the network for any anomalous activity or signs of intrusion □ Depending on the incident, organisations may need to consider higher levels of system logging or network monitoring □ Others: _____
Conducting post-incident review	□ Identify and resolve deficiencies in systems and processes that led to the incident □ Identify and resolve deficiencies in planning and execution of the incident response plan □ Assess if additional security measures are needed to strengthen the security posture of your organisation □ Communicate and build on lessons learnt □ Others: _____ **Revision of the following plans:** □ Prevention and detection plans □ Containment, eradication and recovery plans □ Crisis management and communications plan □ Business continuity plans □ Others: _____

ANNEX D

FLOWCHART FOR DATA BREACH NOTIFICATION



Notification to the PDPC

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

#SGDIGITAL

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.

BROUGHT TO YOU BY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

IN PARTNERSHIP WITH

CSA SINGAPORE