Office of the Victorian Information Commissioner

PRIVACY

Managing the privacy impacts of a data breach

May 2019

Managing the privacy impacts of a data breach

Contents

Part 1: Introduction

Scope and purpose of this guide

This guide is intended to assist organisations that are subject to the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) to prepare for and respond to the privacy implications of data breaches that involve personal information. As a result, you will notice that this document primarily focuses on organisations' obligations from the perspective of potential impacts of data breaches upon individuals (who are the beneficiaries of privacy rights as protected under the PDP Act).

What is a Data Breach?

For the purposes of this guide, a data breach occurs when personal information[1] that is held by a public sector organisation[2] (**organisation**) is subject to misuse or loss or to unauthorised access, modification or disclosure.

Types of Data Breach

A data breach can be caused deliberately as a result of a malicious act from an external or internal party. It can also be caused by human error or by a failure of an organisation to implement effective information management or security systems.

Example

An employee attempts to send correspondence to an individual that has made a complaint to the organisation. The employee, however, inadvertently sends the correspondence to the home address or email address of another complainant.

Example

An organisation's network is 'hacked' by a third party that is then able to access personal information stored on the network.

Example

An employee leaves files or an unsecured laptop containing personal information on public transport.

Example

An organisation publishes details of a new project on its website which includes responses to consultation. Personal information in the responses has been electronically redacted in PDF format but the organisation later discovers that the personal information can be rendered visible where the contents of the PDF are copied and pasted into a Microsoft Word document.

[1] Section 3 of the PDP Act defines personal information as "information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies".

[2] See section 13 for a list of the public sector organisation to which Part 3 of the PDP Act (relating to information privacy) applies.

Consequences of a Data Breach

Privacy is a human right[3] and information privacy (being the protection of personal information) is a key aspect of this right.[4]

It is well understood that the right to privacy can enable the free development of an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life. It is also important to the realisation of other human rights[5] such as the right to freedom of expression[6] and, in extreme circumstances, the right to life[7].

It is not surprising, therefore, that while some data breaches may have no impact or only a minor impact on affected individuals, other data breaches can have serious consequences.

Harm to individuals as a result of a data breach can be physical, financial, emotional or reputational. Some examples of harm arising from a data breach include:

- Reputational damage
- Embarrassment or humiliation
- Emotional distress
- Identity theft or fraud
- Financial loss
- Loss of employment or business opportunities
- Family violence
- Other physical harm and intimidation
- Disruption of government services
- Unwanted marketing and spam email

Organisations can also suffer harm as a result of a data breach. Responding to the initial breach and subsequent complaints may have financial, legal and resource implications. Furthermore, data breaches can result in reputational damage and a loss of public trust.

---

[3] See Article 12 of the *Universal Declaration of Human Rights 1948* (**UDHR**) and Article 17 of the *International Covenant on Civil and Political Rights 1966* (**ICCPR**). In Victoria, the right to privacy is also protected in s 13 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) (**Charter**).

[4] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285, [64] (Bell J).

[5] See for example United Nations General Assembly Resolution 68/167, *The right to privacy in the digital age*, A/RES/68/167 (21 January 2014); United Nations Human Rights Council Resolution 34/7, *The right to privacy in the digital age,* A/HRC/RES/34/7 (7 April 2017).

[6] For example, if an organisation seeks feedback from individuals about local projects but regularly subjects these opinions to unauthorised disclosure, individuals may decide not to express themselves in ways that they otherwise would.

[7] For example, if an individual's life was under threat by a third party and they relocated to avoid harm, a government agency's disclosure of their whereabouts to the third party could have an impact on the individual's right to life.

Part 2: Privacy implications of a data breach

The PDP Act and the Information Privacy Principles

The PDP Act contains 10 Information Privacy Principles (**IPPs**) that underpin how public sector organisations should collect and handle personal information.

As mentioned above, a data breach occurs when personal information held by an organisation is subject to misuse, loss or unauthorised access, modification or disclosure. As such, it will usually involve a failure to comply with one or more of the IPPs and organisations must therefore take steps to address this non-compliance.

We encourage organisations to report data breaches to OVIC even though the PDP Act does not impose any mandatory breach reporting requirement upon organisations when they experience a data breach (see p. 13 -16 below for more guidance on notifying OVIC and individuals affected by a breach).

Other obligations

However, organisations may have obligations under other legal instruments such as under a contract or under other legislation. In this section we focus on:

- The Notifiable Data breach scheme (**NDB Scheme)** or
- the General Data Protection Regulation (**GDPR**).

These schemes will rarely apply to data breaches involving personal information held by Victorian government organisations, but they may apply in certain limited circumstances outlined below.

The Notifiable Data Breaches scheme (NDB scheme)

The **NDB scheme** applies to entities that have obligations to protect the personal information they hold under the *Privacy Act 1988* (Cth) (**Privacy Act**). Entities covered by the Privacy Act include APP entities, credit reporting bodies, credit providers and tax file number (**TFN**) recipients.[8]

The NDB scheme requires these entities to report eligible data breaches (breaches that are likely to result in serious harm) to the Office of the Australian Information Commissioner (OAIC) and to affected individuals.

For the majority of the personal information they hold, Victorian public sector (**VPS**) organisations will not be covered by the NDB scheme. However, many VPS organisations are TFN recipients for the purposes of

[8] See the OAIC's guidance on Entities covered by the NDB scheme at https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#part-4-notifiable-data-breach-ndb-scheme.

the Privacy Act because they receive TFN information for some of their functions.[9] Organisations will therefore need to comply with the NDB scheme if they experience an eligible data breach involving TFN information.

For VPS organisations, an eligible data breach will have the following criteria:

1. There is unauthorised access to or unauthorised disclosure of TFN information.
2. A reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the affected individuals.
3. The organisation has taken remedial action but not been able to prevent the likely risk of serious harm occurring.

When an organisation suspects that an eligible data breach has occurred, the organisation must assess the breach within 30 days to determine whether or not there has been an eligible data breach.[10] If, during the assessment period, the organisation determines that there has been an eligible data breach, the organisation must notify the OAIC and the affected individuals.[11]

The OAIC has produced guidance materials on notifying individuals about an eligible data breach and what should be included in the Notifiable Data Breach statement[12]. This statement must be completed by entities when notifying the OAIC and the affected individuals.

It is considered an interference with the privacy of an individual if the entity does not notify the OAIC of an eligible data breach and the OAIC may therefore decide to exercise enforcement powers under the Privacy Act. For more information on the OAIC Privacy Regulatory Action Policy, organisations should refer to the OAIC's Guide to privacy regulatory action[13].

The EU General Data Protection Regulation (GDPR)

The GDPR is designed to harmonise data privacy laws across the European Union (**EU**) and offer enhanced privacy protections for individuals in the EU. It places an obligation on data controllers[14] to report data breaches to the supervisory authority within 72 hours of the breach occurring. The data controller must also notify data subjects[15] of personal data breaches that are likely to result in a high risk to their rights and freedoms.

---

[9] TFN information is defined in s 6 of the Privacy Act as information that connects a TFN with the identity of a particular individual. A TFN recipient is defined in s 11 of the Privacy Act as any person who is in possession or control of a record that contains TFN information.
[10] See the OAIC's guidance on 'Identifying eligible data breaches' at https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#identifying-eligible-data-breaches.
[11] See the OAIC's guidance on 'Assessing a suspected data breach' at https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#assessing-a-suspected-data-breach.
[12] Available at https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#what-to-include-in-an-eligible-data-breach-statement.
[13] Available at https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/.
[14] Article 4 (7) of the GDPR defines a controller as a natural or legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of processing of personal data
[15] Article 4(1) defines a data subject as an identified or identifiable natural person

The GDPR applies to entities that process the personal data of individuals in the EU, regardless of the location of the entity. Rather, the scope of an organisation's activities will determine the extent to which it will have obligations under the GDPR.
In most cases, GDPR will **not** apply to VPS organisations. However, VPS organisations may have obligations under the GDPR in respect of some of their activities if:

- the organisation offers goods and services to people in the EU, or
- the organisation monitors the behaviour of people in the EU, or
- if the organisation has a physical or legal establishment in the EU[16].

Part 3: Preparing for a Data Breach

One of the main ways that an organisation can minimise the potential negative consequences of a breach for affected individuals and the organisation is to be prepared for them by developing a data breach response plan. This will assist organisations to respond to data breaches quickly and efficiently.

What is a data breach response plan?

The purpose of a data breach response plan is to set out how the organisation will respond to a data breach by walking through what will be done and by whom in the event of a breach.

It is a written document that is directed at all staff of an organisation and which should be approved at the executive level of the organisation. It should be tested (by, for example, applying the plan to a hypothetical data breach) and reviewed regularly to keep it up to date and fit for purpose.

All-staff awareness

The plan should first set out for staff what constitutes a data breach as well as providing examples of data breaches that are relevant to the particular business context of the organisation. This will assist staff in detecting when data breaches occur.

It should explain to staff who they should inform immediately if they suspect that a data breach has occurred (usually the privacy officer or a manager). The plan should also explore the circumstances when a breach can be handled at a managerial level or by the privacy officer alone; when it should be escalated to the data breach response team; and who should make the decision about escalation to the response team.

[16] For further information, see European Data Protection Board's Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (adopted 16 November 2018). Available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

Breach response team

It is the data breach response team that will carry out the steps to minimise the risk of harm associated with the breach (these steps are outlined in Part 3 below) and the plan should set out the membership of the team as well as the roles and responsibilities of its members.

The membership of the breach response team will depend on the context of the organisation (particularly regarding size, resources and skillsets) as well as the nature of the breach. It may be that there is a core membership for all escalated breaches with additional members being involved only when the breach involves their particular area of expertise. Likewise, external experts may be required in some circumstances so organisations should identify what expertise they may need and how it can arrange these services when needed.

A breach response team may include, for example:

- Team Leader – to lead the team and report to the organisation's executive
- Project Manager – to coordinate the work of the team
- Privacy Officer – to provide privacy expertise and breach handling experience
- Information Security – for technical expertise.
- Legal support – to identify legal obligations and offer advice
- IT support – to assist investigations regarding data breaches involving IT systems
- Representative from business area where breach took place – to provide operational information and advice
- Human Resources - to provide advice where the breach involves the actions of a staff member
- Communications– to assist in communicating with affected individuals as well as the media and external stakeholders.

To avoid delays and ensure that the organisation responds to the breach in a timely manner, the breach response team should have the authority to make decisions in carrying out the steps involved in responding to data breaches. This means that it is important that a team leader with sufficient decision-making authority is appointed.

Part 4: Responding to a Data Breach

Key Points

- A breach response consists of **four steps**: Contain, Assess, Notify & Review.
- The overriding principle is **harm minimisation** – minimising potential harm to affected individuals

Overview

The circumstances and risks associated with each breach will be different and, as such, each data breach response needs to be tailored to the particular context. Organisations should, however, act quickly; they should take the breach seriously and treat it as a priority matter requiring immediate resolution. Adopting this approach has the potential to reduce any harm to individuals and negative impact on the organisation.

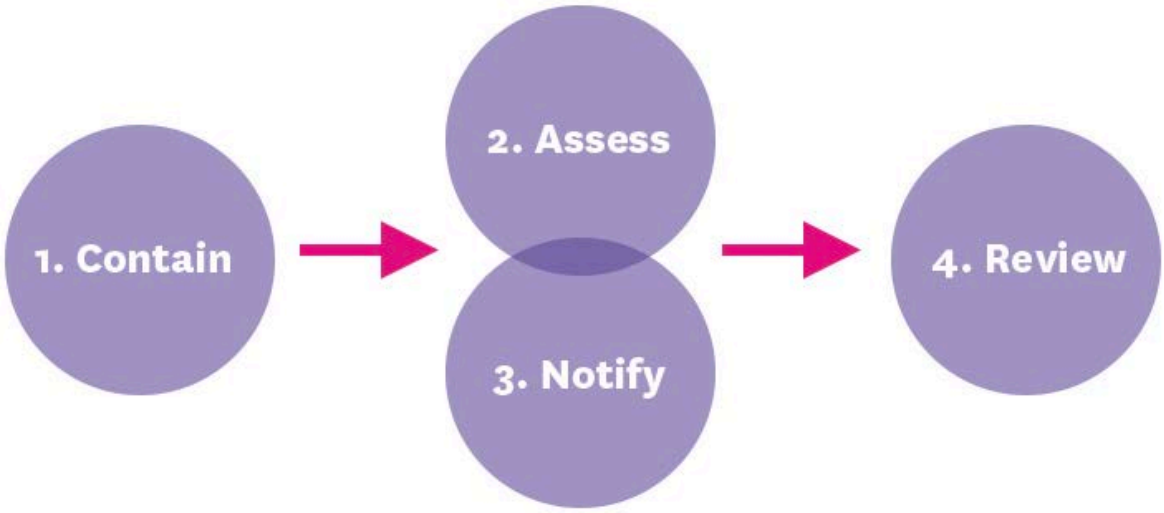
In general, whenever an organisation has identified a data breach and initiated its response plan, its actions should follow four key steps:

Where an organisation identifies potential harm to affected individuals while carrying out these steps, it should make **remediation** attempts at the earliest opportunity to minimise the chances of such harm eventuating (e.g. by relocating an individual where there is a serious threat of physical harm).

1. **Contain** the breach immediately to prevent any further compromise of personal information;
2. **Assess** the risks of harm to affected individuals by investigating the circumstances of the breach;
3. **Notify** affected individuals if deemed appropriate in the circumstances;

Steps 2 & 3 should be taken **simultaneously or in quick succession**.

4. **Review** the breach and the organisation's response to consider longer-term action to prevent future incidents of a similar nature and improve the organisation's handling of future breaches.



Step 1: Contain the breach

Key Points

- It is important to take steps to first confirm that a data breach has occurred.
- Then take immediate measures to limit the extent of the breach.

An organisation should first take steps to confirm that a data breach has occurred. Once confirmed, the organisation should take immediate measures to limit the extent of the breach.

The steps to be taken to contain the breach will depend on the nature of the breach. Some common actions are: stopping the unauthorised practice, recovering the records, shutting down the system that was breached, changing computer access codes or correcting weaknesses in physical or electronic security.

Example:
If an organisation discovers that an ex-employee still has access to the organisation's system and has been accessing the system, to contain the breach the organisation should immediately stop the employee's access.

Example:
An employee intends to send an email to a specific group of employees who work in the same team. The email contains attachments which have the personal information of clients of the team. The employee sends the email to the team but also accidentally sends it to other employees within the organisation who are not part of the team.

To contain this incident, the organisation may attempt to recall the email and, if not possible, get its IT department to attempt to delete the email from the accounts of the unintended recipients. The IT department may also be able to determine whether any of the unintended recipients opened the email before it was deleted and whether they downloaded the attachments. The organisation can then contact the unintended recipients and ask them to delete the email and the attachments.

The organisation's data breach response plan will guide it in deciding who needs to be notified of the incident at this early stage. The data breach response plan will also provide guidance on whether the organisation will need to assemble a data breach response team.

Step 2: Assess the risk of harm

Key Points

- Organisations should assess the **risk of harm** to affected individuals as a result of the breach.
- Risk = **likelihood** and **severity** of harm.
- Assessment of risk will help determine what other response measures are required.

Once organisations have contained a breach (where possible), they should assess the risks of any harm that affected individuals could suffer as a result of the breach. This will require an investigation of the cause of the breach and the surrounding circumstances.

The assessment will assist in determining:

- The measures an organisation should take to remediate any risk of harm;
- Whether and how to notify affected individuals and OVIC about the breach; and
- Steps to take to prevent future breaches.

Factors affecting risk

The risk of harm will depend upon the particular context in each case. It is therefore important that organisations investigate the circumstances of the breach rather than relying upon presumptions or 'one size fits all' type breach responses.

In assessing risk, organisations should consider the severity of any harm that could arise for affected individuals and the likelihood of such harm eventuating. The greater the severity and the greater the likelihood, then the higher the risk.

When assessing the level of risk, organisations should exercise caution if they are in any doubt. For example, if sensitive personal information relating to vulnerable individuals has inadvertently been made publicly available online and it cannot be established who has accessed it, it may be appropriate for the organisation's response to be based off the premise that the information has come into the possession of a third party that could do harm.

Some of the factors to take into consideration when assessing risk are:

- The nature, sensitivity and volume of personal information involved in the data breach
- The circumstances of the data breach, including its cause and extent
- The nature of the potential harm to the affected individuals

The nature, sensitivity and volume of personal information involved in the data breach

Generally speaking, the more sensitive or delicate the personal information, the higher the risk of harm to affected individuals.

Similarly, it is typical that the greater the amount of personal information involved (in terms of both the number of individuals affected and the amount of information pertaining to each individual), the higher the risk of harm.

Example

If an organisation inadvertently published a petition that was submitted to it, the risk of harm in the circumstance of a list of residents petitioning for extra recycling facilities would likely be lower than if the list related to victims of historical sexual abuse petitioning for the prosecution of perpetrators.

The circumstances of the data breach, including its cause and extent

Examining how the breach has occurred can assist in assessing risk. Where a breach has occurred maliciously, it will usually be the case that the risk of harm is higher than where the cause was accidental.

Example
Where personal information has been stolen by a hacker, the risk of harm will usually be higher than if the information was mistakenly sent from one government agency to another government agency.

This also highlights the fact that the recipient and their relationship with the affected individual can have a bearing on the risk of harm eventuating from the breach. Indeed, these factors may be such that personal information that may seem innocuous on the surface is assessed as high risk upon further investigation of the circumstances of the breach.

Example
Where an individual's name and address are accidentally disclosed to a third party, it would usually be appropriate to deem the risk of harm as low risk. However, if the name and address relate to the victim of a violent crime and the unintended recipient is the alleged perpetrator who was awaiting trial then it would be appropriate to rate the risk of harm as being high.

Organisations can also consider any factors that may reduce the risk of harm such as preventative measures or attempts to remediate any potential harm by the organisation.

Example
If an employee loses a USB containing sensitive personal information, the risk of harm will be lessened where the organisation is satisfied that the USB was securely encrypted. If the information was instead contained in a document that was inadvertently leaked online, the risk will be lessened if the organisation removes the document within minutes and is sure that no one has accessed it.

The nature of the potential harm to affected individuals

Organisations should consider the different types of harm (see p. 4 for examples of harm) that could arise as this will impact the level of risk.

Example
Where an individual's email address is inadvertently disclosed and the organisation believes this may result in inconvenience by receiving spam emails, the level of risk will be lower than where a breach involves the disclosure of information that exposes the individual to identity theft.

The particular characteristics and circumstances of the individuals affected may also impact the risk of harm. This is particularly the case for vulnerable individuals as where their personal information is compromised, they may be placed at greater risk of harm than what otherwise could be expected

Step 3: Notify Affected Individuals

Key points

- If there is a foreseeable risk of harm arising from the data breach then affected individuals should be notified.
- Notification may not be appropriate if it is reasonably likely to cause more harm than it would alleviate.
- Notifying OVIC of data breaches is strongly encouraged.

Whether or not an organisation chooses to notify affected individuals of a data breach will largely be determined by the outcome of the risk assessment carried out in Step 2.

Notification is particularly important where it would mitigate potential harm that may arise from the incident. Notification may allow individuals to take steps to prevent any harm from arising as a result of the breach.

Whether to notify affected individuals

When deciding whether to notify affected individuals about a data breach, the organisation should consider:

- The foreseeable risk of harm to affected individuals.
- Contractual and other legal obligations.

Foreseeable risk of harm to affected individuals

When deciding whether to notify, the main factor to consider is whether there is a foreseeable risk of harm to the affected individuals.

Organisations should notify individuals where there is a foreseeable risk of harm. If an organisation is unsure about whether there is a foreseeable risk of harm, it may be best to exercise caution and notify the affected individuals. Notification is aimed at allowing individuals to take steps to minimise any potential harm from the breach.

Notification may not be necessary where the organisation has determined that there is no risk of harm or the risk of harm is too remote to be of real concern.

Similarly it may not be appropriate to notify individuals where notification is reasonably likely to cause more harm than it would alleviate[17] such as where notification may cause undue stress or anxiety to the affected individuals.

[17] See Office of the Victorian Privacy Commissioner, Report 01.06 J*enny's case: Report of an investigation into the Office of Police Integrity pursuant to Part 6 of the Information Privacy Act 2000*, February 2006. Available at https://www.parliament.vic.gov.au/papers/govpub/VPARL2003-06No166.pdf.

Example:
A University sends an email to a specific group of students for a specific purpose. However, accidentally attached to the email is a spreadsheet with the personal and sensitive information of other students.

The affected students should be notified of the breach as there are a number of risks arising from this incident including identity theft and reputational harm.

Example:
An organisation becomes aware that a subset of its database, containing the personal information of clients who access its family violence services, has accidentally been made publicly accessible on the internet due to a technical error.

After fixing the error, the organisation determines that the information was publicly available for two weeks but is unable to determine whether it was accessed by anyone. Whilst there is a possibility that no one accessed the information, the organisation decides that it should notify the affected individuals given the high risk of harm that could be caused if the information was accessed.

Example
A Council employee loses a bag whilst on Council premises. The bag contains documents that include personal information of an individual that receives council services. The Council reports the missing bag to the police but the bag is retrieved around an hour later by another Council employee.

After conducting enquiries, the Council is satisfied that there has been no unauthorised access to the documents containing personal information and decides not to notify the individual.

Legal or contractual obligations to notify

Organisations should consider whether they are obliged to notify affected individuals or other bodies under legislation other than the PDP Act or under contract. Two scenarios where these obligations may arise are covered above in relation to the NDB scheme and GDPR.

When to notify

Organisations should notify affected individuals as soon as reasonably possible after the breach has been contained and assessed.

It is important for the organisation to gather enough information about the data breach so that the notification is sufficiently detailed.

To avoid undue delay in notification, In complex matters it may be appropriate to provide affected individuals with information in stages, as the organisation becomes aware of more information.

In some circumstances, it may be necessary to delay notification. If, for example, a law enforcement agency is involved in investigating matters related to the breach, it may be appropriate to consult the agency before notifying affected individuals of the incident.

How to notify

Organisations should usually notify individuals directly (by phone, email, letter or in person). Where it is not practicable to do so (such as where the organisation does not have the contact details for affected individuals) then it may provide notification indirectly by, for example, publishing a notice on its website or making a media announcement.

Depending on the nature of the breach, it may be appropriate to use multiple methods of notification. For example, an organisation may choose to meet with vulnerable clients affected by a data breach and to also provide a written notification that those clients can refer back to.

If the breach involves multiple agencies or a contract with a third party, it should usually be the organisation that has the most direct relationship with the individual that should provide notification. Organisations should address responsibility for data breach management and reporting in their contracts with third party providers.

Content of the notification

The content of the notification will vary depending on the nature of the breach and the method of notification chosen. Generally, the notification should have enough information for the affected individuals to understand the circumstances of the breach, the possible impacts of the breach and the organisation response efforts.
A notification should include, as appropriate:

- A description of the data breach including when it occurred.
- A description of the personal information involved in the breach.
- The steps the organisation has taken, or is taking, to contain the incident and minimise any potential harm arising from the incident.
- The steps the affected individuals can take to reduce or avoid the risk of harm.
- Contact information of an individual or a department within your organisation that affected individuals can speak to about the incident.
- The OVIC contact information and advice that affected individuals have a right of complaint to OVIC if they are not satisfied with the organisation's response to their direct complaint.

The notification should be written in plain English so that it is clear and easy to understand. It should avoid complex terms or technical jargon.

Notifying OVIC

Organisations are encouraged to notify OVIC of data breaches that may involve a foreseeable risk of harm as soon as reasonably possible. There are a number of good reasons to do so:

- OVIC can provide guidance to your organisation on how to minimise any privacy risks arising from the incident.
- OVIC will be able to respond more effectively to enquiries and complaints from individuals who have been affected by the data breach.
- Proactively engaging with OVIC about a data breach will generally make it less likely that we will take formal regulatory action in respect of the matter.

There is no required form or format when notifying the OVIC of a data breach. Your organisation may decide to notify via phone in the preliminary stages to discuss the incident and then provide a written report when all the breach response stages have been finalised. There is a reporting template in Part 4 of this document which organisations may find helpful when preparing their written notification to OVIC.

Step 4: Review

Key points

- Reviewing a data breach incident allows an organisation to implement key learnings that will improve its data breach response process.
- Reviewing a data breach incident also helps an organisation to identify areas of improvement in its information handling practices.

When the organisation has handled the privacy impacts of the particular breach, it should then conduct a review of the data breach and identify appropriate measures to implement that will prevent, or reduce the chances of, similar incidents occurring in the future.

A review of the incident may involve:

- A security audit of both physical and technical security.
- A review of relevant policies, practices and procedures and making changes to reflect the lessons learned from the review.
- A review of employee training practices.
- A review of contractual obligations imposed on contracted service providers.
- An audit to ensure the prevention plan is implemented.

This step will require an assessment of the root cause of the breach so that the organisation identifies what it can do to prevent a similar incident occurring again. It is important to be aware that there may be several causes of the breach.

Example:

A staff member loses a USB stick containing clients' personal information resulting in some of those clients becoming a victim of identity fraud.

While this breach involves an element of human error, the fact that the USB stick was not encrypted contributed to the data breach. The organisation can review its policies and procedures around the use of USB sticks and change its policy so that staff are required to use USB sticks that are encrypted.

OVIC's *Guidelines to protecting the security of personal information*[18] is a useful resource for organisations when reviewing their information management practices and data breach response processes.

Organisations should also evaluate how well it responded to the breach and make any necessary changes to its breach response plan as a result.

[18] See: https://ovic.vic.gov.au/resource/guidelines-to-protecting-the-security-of-personal-information-reasonable-steps-under-information-privacy-principle-4-1/.

Part 5: Template for reporting a breach to OVIC

Please provide as much detail as you can. However, we encourage organisations to contact OVIC as soon as reasonably possible so that we may offer advice where appropriate and so we can respond from to any enquiries relating to the breach. We therefore recognise that you may not have all the information at the time that you report to OVIC.

Question	Details (if known)
What happened?	
When did it happen and when did organisation become aware of it?	
What personal information is involved?	
How did it happen? - who caused the breach? - was it malicious or accidental? - who has accessed the information in unauthorised manner?	
What is the risk of harm? - what type of harm? - how serious? - how likely?	
Steps taken or proposed to contain breach.	
Have affected individuals been notified? - if not, why? - If so, how? What reactions?	
Steps taken or proposed to prevent future breaches	
Any other information	