Australian Government

Office of the Australian Information Commissioner

Data breach preparation and response

A guide to managing data breaches in accordance with the *Privacy Act 1988* (Cth)

oaic.gov.au

OAIC

February 2018

Foreword

Strong data management is integral to the operation of businesses and government agencies worldwide. Digital platforms and technologies that utilise user data to provide personalised products or services have proliferated across communities and industries. At the same time, data analysis has been widely recognised for its value as fuel for innovation that can benefit the community in unprecedented ways, including identifying gaps in services, revealing needs for new or different products, and enabling better-informed policy-making.

In this environment, the success of an organisation that handles personal information or a project that involves personal information depends on trust. People have to trust that their privacy is protected, and be confident that personal information will be handled in line with their expectations.

As we've found in our long-running national community attitudes to privacy survey, if an organisation does not demonstrate a commitment to privacy, people will look for alternative suppliers, products, and services.

One of the biggest risks organisations face in this context is a data breach. A data breach involving personal information can put affected individuals at risk of serious harm and consequently damage an organisation's reputation as a data custodian.

However, it is important to recognise that consumer and community trust is not necessarily extinguished immediately after a data breach occurs. After all, history has shown us that even organisations with great information security can fall victim to a data breach, due to the rapid evolution of data security threats and the difficulty of removing the risk of human error in large and complex organisations.

When a data breach occurs, a quick and effective response can have a positive impact on people's perceptions of an organisation's trustworthiness. That is why being prepared for a data breach is important for all organisations that handle personal information.

By an 'effective' response to a data breach, I mean a response that successfully reduces or removes the risk of harm to individuals, and which aligns with legislative requirements and community expectations.

This guide aims to assist you in developing and implementing an effective data breach response. It outlines the requirements relating to data breaches in the *Privacy Act 1988* (Cth) (Privacy Act), including personal information security requirements and the mandatory data breach reporting obligations of the Notifiable Data Breaches (NDB) scheme. The guide also covers other key considerations in developing a robust data breach response strategy, including the key steps to take when a breach occurs, the capabilities of staff, and governance processes.

While this guide is primarily for Australian Government agencies and private sector organisations with obligations under the Privacy Act, the information provided is useful to any organisation

operating in Australia. Taken holistically, the information provided in this guide provides a framework for meeting expectations for accountability and transparency in data breach prevention and management, which is key to maintaining and building consumer and community trust.

Timothy Pilgrim PSM

Australian Information Commissioner
Australian Privacy Commissioner

Contents

Purpose and structure of this guide

The Office of the Australian Information Commissioner (OAIC) has prepared this guide to assist Australian Government agencies and private sector organisations (entities) prepare for and respond to data breaches in line with their obligations under the *Privacy Act 1988* (Cth) (Privacy Act).

The guide is in five parts.

Part 1: Data breaches and the Australian Privacy Act

This section outlines the requirements of the Privacy Act that relate to personal information security and data breach response strategy. The principles contained within the Privacy Act for the handling of personal information may be adopted by any entity to lower the risk of a data breach occurring and to effectively reduce the impact of a data breach.

Part 2: Preparing a data breach response plan

The faster an entity responds to a data breach, the more likely it is to effectively limit any negative consequences. A data breach response plan is essential to facilitate a swift response and ensure that any legal obligations are met following a data breach.

Part 3: Responding to data breaches — Four key steps

An effective data breach response generally follows a four-step process — contain, assess, notify, and review. This section outlines key considerations for each of these steps to assist entities in preparing an effective data breach response.

Part 4: Notifiable Data Breaches

This section outlines the requirements of the NDB scheme under the Privacy Act. The NDB scheme contains mandatory data breach reporting obligations in relation to certain data breaches, and requirements to assess suspected data breaches.

Part 5: Other sources of information

The obligations of the Privacy Act in relation to data breaches co-exist with other reporting obligations. This section assists entities in identifying where they can find information about other data breach reporting requirements.

Who should use this guide?

Any entity that handles personal information can use this guide to inform their preparation and response strategy for a data breach.

However, this guide is primarily targeted at entities that have obligations under the Privacy Act to protect personal information. These entities are required to take reasonable steps to protect the personal information that they hold, and may be required to notify affected individuals and the Australian Information Commissioner (Commissioner) of a data breach under the NDB scheme.

How to use this guide

Different parts of this guide will be of greater or lesser relevance to different entities depending on their goals.

Entities seeking a greater understanding of the Privacy Act, specifically in how the Privacy Act's requirements relate to personal information security and data breach management responsibilities, should refer primarily to Part 1 and Part 4.

Entities that want to prepare a data breach response strategy, or review the effectiveness of their current response plan, should refer primarily to Part 2 and Part 3.

Entities that have experienced a data breach can refer to Part 3 to understand the main components of an effective data breach response. They should also refer to Part 4, as it provides guidance on the mandatory data breach reporting and assessment requirements of the NDB scheme.

A cautionary note

There is no 'one size fits all' solution to preparing for and responding to data breaches. This guide does not provide detailed information about the systems or processes an entity may put in place to manage data breaches.

Further, this guide does not provide detailed information about other obligations that may apply to entities in addition to the Privacy Act. Entities should consider their privacy obligations alongside other relevant legal requirements and standards.

The guide does not constitute or replace legal advice on obligations under the Privacy Act. It is published by the Commissioner to provide general information to help entities meet the requirements of the Privacy Act. Entities are encouraged to seek professional advice tailored to their own circumstances where required.

Part 1: Data breaches and the Australian Privacy Act

Key points

- A data breach is an unauthorised access or disclosure of personal information, or loss of personal information.
- Data breaches can have serious consequences, so it is important that entities have robust systems and procedures in place to identify and respond effectively.
- Entities that are regulated by the Privacy Act should be familiar with the requirements of the NDB scheme, which are an extension of their information governance and security obligations.
- A data breach incident may also trigger reporting obligations outside of the Privacy Act.

What is a data breach?

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable.[1] Entities should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

Consequences of a data breach

Data breaches can cause significant harm in multiple ways.

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of harm include:

[1] Section 6 of the Privacy Act. For detailed information about the scope of 'personal information', see the OAIC's guide *What is personal information?* [www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information].

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence
- physical harm or intimidation.

A data breach can also negatively impact an entity's reputation for privacy protection, and as a result undercut an entity's commercial interests. As shown in the OAIC's long-running national community attitudes to privacy survey, privacy protection contributes to an individual's trust in an entity. [2] If an entity is perceived to be handling personal information contrary to community expectations, individuals may seek out alternative products and services.

An entity can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that an entity takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in an entity's personal information handling capability.

The Australian Privacy Principles

The Privacy Act contains 13 Australian Privacy Principles (APPs) that set out entities' obligations for the management of personal information. The APPs are principles-based and technologically neutral; they outline principles for how personal information is handled and these principles may be applied across different technologies and uses of personal information over time.

Compliance with the APPs as a whole will reduce the risk of a data breach occurring. This is because the APPs ensure that privacy risks are reduced or removed at each stage of personal information handling, including collection, storage, use, disclosure, and destruction of personal information. For example, APP 3 restricts the collection of personal information. APPs 4.3 and 11.2 outline requirements to destroy or de-identify information if it is unsolicited or no longer needed by the entity. Compliance with these requirements reduces the amount of data that may be exposed as a result of a breach.

Compliance with the requirement to secure personal information in APP 11 is key to minimising the risk of a data breach.[3] APP 11 requires entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. The type of steps that are reasonable to protect information will

---

[2] See the OAIC's webpage: https://www.oaic.gov.au/engage-with-us/community-attitudes/.

[3] Sections 20Q and 21S of the Privacy Act impose equivalent obligations on credit reporting agencies and all credit providers. Similarly, the *Privacy (Tax File Number) Rule 2015* [www.legislation.gov.au/Details/F2015L00249] made under s 17 of the Privacy Act requires TFN recipients to take reasonable steps to protect TFN information from misuse and loss, and from unauthorised access, use, modification or disclosure.

depend on the circumstances of the entity and the risks associated with personal information handled by the entity.[4]

In addition, APP 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the APPs.[5]

The OAIC has published various resources to assist entities to meet their obligations under APP 1.2[6] and APP 11.[7]

The Notifiable Data Breaches (NDB) scheme

The NDB scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Commissioner of certain data breaches.

The NDB scheme requires entities to notify individuals and the Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm. For example, an individual can change passwords to compromised online accounts, and be alert to identity fraud or scams.

The NDB scheme also serves the broader purpose of enhancing entities' accountability for privacy protection. By demonstrating that entities are accountable for privacy, and that breaches of privacy are taken seriously, the NDB scheme works to build trust in personal information handling across industries.

---

4 See Chapter 11 of the *APP Guidelines* [www.oaic.gov.au/agencies-and-organisations/app-guidelines/] and the *Guide to securing personal information* [www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information].

5 A similar requirement applies to credit reporting bodies in s 20B(2), to take reasonable steps to implement practices, procedures and systems to ensure compliance with the credit reporting obligations in Part IIIA of the Privacy Act and the *Privacy (Credit Reporting) Code 2014 (Version 1.2)* [www.legislation.gov.au/Details/F2014L00459].

6 See *Privacy Management Framework* and *Privacy management plan template* [www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-plan-template], and Chapter 1 of the *APP Guidelines* [www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information].

7 See Chapter 11 of the APP Guidelines [www.oaic.gov.au/agencies-and-organisations/app-guidelines/] and the *Guide to securing personal information* [www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information].

Part 4 of this guide provides detailed information to assist entities to meet their obligations under Part IIIC of the Privacy Act when responding to an eligible data breach or a suspected eligible data breach.

Other obligations

Entities may have other obligations outside of those contained in the Privacy Act that relate to personal information protection and responding to a data breach. These may include other data protection obligations under state-based or international data protection laws. Australian businesses may need to comply with the European Union's (EU's) General Data Protection Regulation (GDPR)[8] if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU.

For data breaches affecting certain categories of information, other mandatory or voluntary reporting schemes may exist. For example, entities might consider reporting certain breaches to:

- the entity's financial services provider
- police or law enforcement bodies
- the Australian Securities & Investments Commission (ASIC)
- the Australian Prudential Regulation Authority (APRA)
- the Australian Taxation Office (ATO)
- the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- the Australian Cyber Security Centre (ACSC)
- the Australian Digital Health Agency (ADHA)
- the Department of Health
- State or Territory Privacy and Information Commissioners
- professional associations and regulatory bodies
- insurance providers.

Links to other resources are contained in Part 5 of this guide.

Some entities may have additional obligations to report to the Commissioner under the *National Cancer Screening Register Act 2016* (NCSR Act) or have different reporting obligations under the *My Health Records Act 2012* (My Health Records Act).

Under the NCSR Act, current and former contracted service providers of the National Cancer Screening Register must notify the Secretary of the Department of Health (the Secretary) and the Commissioner if they become aware of unauthorised recording, use or disclosure of personal information included in the Register. The Secretary must also notify the Commissioner of certain data breaches, including potential breaches, in connection with the National Cancer Screening Register. The Secretary must also consult the Information Commissioner about notifying individuals who may be affected. Separately, entities with NCSR Act obligations must consider

[8] The OAIC's *Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation* [www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation] may assist Australian businesses to understand and comply with the GDPR's requirements. Further guidance is also available from the Article 29 Working Group [http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936].

whether the incident also requires notification under the NDB scheme, as the two schemes operate concurrently. Where the test for both schemes have been met, the entity may make a joint notification to the Commissioner.

Certain participants in the My Health Record system (such as the System Operator, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider), are required to report data breaches that occur in relation to the My Health Record system to the either the System Operator or the Commissioner, or both, depending on the entity reporting the data breach (s 75 of the My Health Records Act). More information about obligations under the My Health Records Act and how these obligations interact with the NDB scheme is available in Part 4.

Part 2: Preparing a data breach response plan

Key points

- A quick response to a data breach, based on an up-to-date data breach response plan, is critical to effectively managing a breach
- your data breach response plan should outline your entity's strategy for containing, assessing and managing the incident from start to finish
- this part will provide practical guidance to help you develop a comprehensive and effective data breach response plan.

Why do you need a data breach response plan?

All entities should have a data breach response plan. A data breach response plan enables an entity to respond quickly to a data breach. By responding quickly, an entity can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

A data breach response plan can help you:

- **Meet your obligations under the Privacy Act**

Under the Privacy Act, an entity must take reasonable steps to protect the personal information that it holds.[9] A data breach response plan focussed on reducing the impact of a breach can be one of these reasonable steps.

- **Limit the consequences of a data breach**

A quick response can reduce the likelihood of affected individuals suffering harm. It can also lessen financial or reputational damage to the entity that experienced the breach.

- **Preserve and build public trust**

An effective data breach response can support consumer and public confidence in an entity's respect for individual privacy, and the entity's ability to manage personal information in accordance with community expectations.

What is a data breach response plan?

A data breach response plan is a framework that sets out the roles and responsibilities involved in managing a data breach. It also describes the steps an entity will take if a data breach occurs.

---

[9] An APP entity is required under s 15 not to do an act, or engage in a practice, that breaches APP 11.1; a credit reporting body is required to comply with s 20Q in relation to credit reporting information; a credit provider is required to comply with s 21S(1) in relation to credit eligibility information; a file number recipient is required under s 18 not to do an act, or engage in a practice, that breaches the *Privacy (Tax File Number) Rule 2015* [www.legislation.gov.au/Details/F2015L00249].

Your data breach response plan should be in writing to ensure that your staff clearly understand what needs to happen in the event of a data breach. It is also important for staff to be aware of where they can access the data breach response plan on short notice.

You will need to regularly review and test your plan to make sure it is up to date and that your staff know what actions they are expected to take. You can test your plan by, for example, responding to a hypothetical data breach and reviewing how your response could be made more effective.

How regularly you test your plan will depend on your circumstances, including the size of your entity, the nature of your operations, the possible adverse consequences to an individual if a breach occurs, and the amount and sensitivity of the information you hold. It may be appropriate in some instances that a review of the plan coincides with the introduction of new products, services, system enhancements, or such other events which involve the handling of personal information.

What should the plan cover?

The more comprehensive your data breach response plan is, the better prepared your entity will be to effectively reduce the risks and potential damage that can result.

Information that your plan should cover includes:

- **A clear explanation of what constitutes a data breach**

This will assist your staff in identifying a data breach should one occur (see *What is a data breach?* section above). You may also want to include potential examples of a data breach which are tailored to reflect your business activities.

- **A strategy for containing, assessing and managing data breaches**

This strategy should include the actions your staff, and your response team, will take in the event of a data breach or a suspected data breach. Consider:

  - potential strategies for containing and remediating data breaches
  - ensuring you have the capability to implement those strategies as a matter of priority (e.g. having staff available to deal with the breach – see *Response team membership* section below). Your plan should reflect the capabilities of your staff to adequately assess data breaches and their impact, especially when breaches are not escalated to a response team
  - legislative or contractual requirements (such as the requirements of the NDB scheme if they apply to your entity)
  - a clear and immediate communications strategy that allows for the prompt notification of affected individuals and other relevant entities. In particular:
    - who is responsible for implementing the communications strategy
    - determining when affected individuals must be notified (refer to *Identifying eligible data breaches* for further information about mandatory data breach notification requirements under the NDB scheme)
    - how affected individuals will be contacted and managed
    - criteria for determining which external stakeholders should be contacted (for example, law enforcement and cyber security agencies, regulators such as the OAIC, and the media)

- who is responsible for liaising with external stakeholders.

- **The roles and responsibilities of staff**

Your plan should outline the responsibilities of staff members when there is a data breach, or a suspected data breach. Consider:

- who staff should inform immediately if they suspect a data breach
- the circumstances in which a line manager can handle a data breach, and when a data breach must be escalated to the response team. The following factors may determine when a data breach is escalated to the response team:
  - the number of people affected by the breach or suspected breach
  - whether there is a risk of serious harm to affected individuals now or in the future
  - whether the data breach or suspected data breach may indicate a systemic problem with your entity's practices or procedures
  - other issues relevant to your circumstances, such as the value of the data to you or issues of reputational risk.
- who is responsible for deciding whether the breach should be escalated to the response team. One option is for each senior manager to hold responsibility for deciding when to escalate a data breach to the response team. Another option is to have a dedicated role, such as the privacy contact officer.

- **Documentation**

  Your plan should consider how your entity will record data breach incidents, including those that are not escalated to the response team. This will assist you in ensuring you have documentation of how your entity has met regulatory requirements.

- **Review**

  Evaluating how a data breach occurred, and the success of your response, can help you improve your data handling and data breach management. Consider:

  - a strategy to identify and address any weaknesses in data handling that contributed to the breach
  - a system for a post-breach assessment of your entity's response to the data breach and the effectiveness of your data breach response plan.

Response team membership

Your data breach response team is responsible for carrying out the actions that can reduce the potential impact of a data breach. It is important that the staff that make up the response team, as well as their roles and responsibilities, are clearly established and documented before a data breach occurs. Otherwise, your response to the breach may be unnecessarily delayed.

Who is in your data breach response team will depend on the circumstances of your entity and the nature of the breach. Different skill sets and staff may be needed to respond to one breach compared to another. In some cases, you may need to include external experts in your team, for example legal advice, data forensics, or media management. You should identify the types of

expertise you may need and ensure that this expertise will be available on short notice. You might consider creating a core team and adding other members as they are required.

You should keep a current list of response team members and clearly detail their roles, responsibilities, and authorities, as well as their contact details (possibly attached to the data breach response plan). You should ensure these contact details remain updated, particularly in the event of organisational changes. Each role on the response team should have a second point of contact in case the first person is not available.

Typical data breach response team roles and skills

Your data breach response team may include:

- a team leader — who is responsible for leading the response team and reporting to senior management
- a project manager — to coordinate the team and provide support to its members
- a senior member of staff with overall accountability for privacy and/or key privacy officer — to bring privacy expertise to the team
- legal support — to identify legal obligations and provide advice
- risk management support — to assess the risks from the breach
- Information and Communication Technology (ICT) support/forensics support — this role can help establish the cause and impact of a data breach that involved ICT systems
- information and records management expertise – to assist in reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs) and to provide advice on recording the response to the data breach
- human resources (HR) support — if the breach was due to the actions of a staff member
- media/communications expertise — to assist in communicating with affected individuals and dealing with the media and external stakeholders.

If you hold an insurance policy for data breaches, that insurer may have a pre-established panel of external service providers in many of the roles listed above. You may want to consult with your insurer as to the identity of that panel so they can be included in any response team. Alternatively, the insurer may have a hotline available to assist in the event of a data breach, and that could be noted in the response plan.

Which individuals carry out the roles outlined in your response team will depend on your circumstances. For example, in smaller entities it may not be necessary to include steps related to escalating the data breach to the response team, as this may be an automatic process. Depending on the size of your entity or the size of the breach, a single person may perform multiple roles. In smaller entities the owner/principal of the entity could potentially be the person who needs to respond to and act on that breach.

It is important that the response team has the authority to take the steps outlined in the response plan without needing to seek permission, as this will enable a faster response to the breach. The role of team leader should be carefully considered, as they should have sufficient ability and authority to effectively manage the various sections within the entity whose input is required and to report to senior management. It may be your senior member of staff with overall accountability

for privacy, a senior lawyer (if you have an internal legal function) or another senior manager. If the breach is serious, it may be a senior executive.

Actions the response team should take

A data breach response plan should also set out (or refer to) the actions the response team is expected to take when a data breach is discovered. Part 3 of this Guide provides a general framework for responding to a data breach, and Part 4 outlines the requirements of the NDB scheme, which may apply to your entity if they have personal information security obligations under the Privacy Act.

The response team will need to consider what information needs to be reported to senior management and at what point. This reporting structure should form part of the plan.

The data breach response plan should outline how staff will record how they have become aware of a data breach and the actions taken in response. Keeping records on data breaches and suspected breaches will help you manage the breach and identify risks that could make a breach more likely to occur.

Other considerations

In developing your plan you could also consider:

- when and how the response team could practice a response to a breach in order to test procedures and refine them
- whether your plan for dealing with personal information data breaches could link into or be incorporated into already existing processes, such as a disaster recovery plan, a cyber security/ICT incident response plan, a crisis management plan or an existing data breach response plan involving other types of information (e.g. commercially confidential information)
- whether senior management should be directly involved in the planning for dealing with data breaches and in responding to serious data breaches
- any reporting obligations under laws other than the Privacy Act or to other entities
- whether you have an insurance policy for data breaches that includes steps you must follow.

Data breach response plan quick checklist

Use this list to check whether your response plan addresses relevant issues.

Information to be included	Yes/No	Comments
What a data breach is and how staff can identify one		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsibilities		
Details of any external expertise that should be engaged in particular circumstances		
How the plan will apply to various types of data breaches and varying risk profiles with consideration of possible remedial actions		
An approach for conducting assessments		
Processes that outline when and how individuals are notified		
Circumstances in which law enforcement, regulators (such as the OAIC), or other entities may need to be contacted		
Processes for responding to incidents that involve another entity		
A record-keeping policy to ensure that breaches are documented		
Requirements under agreements with third parties such as insurance policies or service agreements		
A strategy identifying and addressing any weaknesses in data handling that contributed to the breach		
Regular reviewing and testing of the plan		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach response plan		

Part 3: Responding to data breaches — four key steps

Key points

- Each data breach response needs to be tailored to the circumstances of the incident.
- In general, a data breach response should follow four key steps: contain, assess, notify and review.

Overview

Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and entities.

As such, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

Generally, the actions taken following a data breach should follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

At any time, entities should take remedial action, where possible, to limit the impact of the breach on affected individuals. If remedial action is successful in preventing a likely risk of serious harm to individuals, the NDB scheme notification obligations may not apply.

In general, entities should:

- take each data breach or suspected data breach seriously and move immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed
- undertake steps 1 (Contain), 2 (Assess), and 3 (Notify) either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs
- determine how to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, an entity may take additional steps that are specific to the nature of the breach.

The following diagram summarises the data breach response process. The parts of this process that are required by the NDB scheme are coloured red. The NDB scheme is explained in detail in Part 4 of this guide.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — Is serious harm still likely? — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Step 1: Contain

Once an entity has discovered or suspects that a data breach has occurred, it should immediately take action to limit the breach.

For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Addressing the following questions may help you identify strategies to contain a data breach:

- How did the data breach occur?
- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

At this point, an entity may suspect an eligible data breach under the NDB scheme has occurred, which would trigger assessment obligations. Or, the entity may believe the data breach is an eligible data breach, which requires them to notify individuals as soon as practicable.

During this preliminary stage, be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable the entity to address all risks posed to affected individuals or the entity.

Step 2: Assess

An assessment of the data breach can help an entity understand the risks posed by a data breach and how these risks can be addressed. It should be conducted as expeditiously as possible.

Gather and evaluate as much information about the data breach as possible. By creating a complete picture of the data breach, an entity can ensure they understand the risk of harm to affected individuals, and identify and take all appropriate steps to limit the impact of a data breach.

This assessment should also assist entities in deciding whether affected individuals must be notified.

In your assessment of a data breach, consider:

- the type or types of personal information involved in the data breach
- the circumstances of the data breach, including its cause and extent
- the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

All entities should consider whether remedial action can be taken to reduce any potential harm to individuals. This might also take place during Step 1: Contain, such as by recovering lost information before it is accessed.

Entities subject to the NDB scheme are required to conduct an assessment of 'suspected' eligible data breaches and take reasonable steps to complete this assessment within 30 days (see *Assessing a suspected data breach*). Criteria for assessing a data breach, including the risk of harm and remedial action, is explored in *Identifying eligible data breaches*.

Step 3: Notify

Notification can be an important mitigation strategy that has the potential to benefit both the entity and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. Sometimes, notifying individuals can cause undue stress or harm. For example, notifying individuals about a data breach that poses very little or no risk of harm can cause unnecessary anxiety. It can also de-sensitise individuals so that they don't take a notification seriously, even when there is a real risk of serious harm. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

Consider:

- the obligations of the entity under the NDB scheme. Entities are required to notify individuals and the Commissioner about data breaches that are likely to result in serious harm. Part 4 of this guide provides further detail about the NDB scheme's requirements
- other circumstances in which individuals should be notified. For example, your entity may not have obligations under the NDB scheme, but have processes in place to notify affected individuals in certain circumstances
- how notification should occur, including:
  - what information is provided in the notification
  - how the notification will be provided to individuals
  - who is responsible for notifying individuals and creating the notification.
- who else other than affected individuals (and the Commissioner if the notification obligations of the NDB scheme apply) should be notified
- where a law enforcement agency is investigating the breach, it may be appropriate to consult the investigating agency before making details of the breach public
- whether the incident triggers reporting obligations to other entities.

Effective data breach response is about reducing or removing harm to affected individuals, while protecting the interests of your organisation or agency. Notification has the practical benefit of providing individuals with the opportunity to take steps to protect their personal information following a data breach, such as by changing account passwords or being alert to possible scams resulting from the breach. It is important that staff are capable of engaging with individuals who have been affected by a data breach with sensitivity and compassion, in order not to exacerbate or cause further harm. Notification can also help build trust in an entity, by demonstrating that privacy protection is taken seriously.

Step 4: Review

Once steps 1 to 3 have been completed, an entity should review and learn from the data breach incident to improve its personal information handling practices.

This might involve:

- a security review including a root cause analysis of the data breach
- a prevention plan to prevent similar incidents in future
- audits to ensure the prevention plan is implemented
- a review of policies and procedures and changes to reflect the lessons learned from the review
- changes to employee selection and training practices
- a review of service delivery partners that were involved in the breach.

In reviewing information management and data breach response, an entity can refer to the OAIC's *Guide to securing personal information*.[10]

When reviewing a data breach incident, it is important to use the lessons learned to strengthen the entity's personal information security and handling practices, and to reduce the chance of reoccurrence. A data breach should be considered alongside any similar breaches that have occurred in the past, which could indicate a systemic issue with policies or procedures.

If any updates are made following a review, staff should be trained in any changes to relevant policies and procedures to ensure a quick response to a data breach.

[10] Available online at www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

Part 4: Notifiable Data Breach (NDB) Scheme

The Privacy Act requires certain entities to notify individuals and the Commissioner about data breaches that are likely to cause serious harm.

The requirements of the NDB scheme are contained in Part IIIC of the Privacy Act and apply to breaches that occur on or after 22 February 2018.

This part of the guide covers the following topics:

- Entities covered by the NDB scheme
- Data breaches involving more than one entity
- Identifying eligible data breaches
- Exceptions to the notification obligation
- Assessing a suspected data breach
- Notifying individuals about an eligible data breach
- What to include in an eligible data breach statement
- The Australian Information Commissioner's role in the NDB scheme.

Entities covered by the NDB scheme

Key points

- Entities that have existing obligations under the Privacy Act to secure personal information must comply with the NDB scheme.
- This includes Australian Government agencies, businesses and not-for profit organisations that have an annual turnover of more than AU$3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information and tax file number (TFN) recipients.
- Entities that have Privacy Act security obligations in relation to particular types of information only (for example, small businesses that are required to secure tax file number information) do not need to notify about data breaches that affect other types of information outside the scope of their obligations under the Privacy Act.

APP entities

The NDB scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold (s 26WE(1)(a)).[11] Collectively known as 'APP entities', these include Australian Government agencies and private sector and not-for-profit organisations with an annual turnover of more than $3 million. The definition of APP entity generally does not include small business operators, registered political parties, state or territory authorities, or a prescribed instrumentality of a state (s 6C). However, some businesses of any size are APP entities, including businesses that trade in personal information[12] and organisations that provide a health service to, and hold health information about, individuals (see *Is my organisation a health service provider?*).[13]

For more information about APP entities, see Chapter B of the *Australian Privacy Principle Guidelines* (APP Guidelines).[14]

Exempt acts and practices, including employee records

The NDB scheme only applies to entities and personal information holdings that are already subject to security requirements under the Privacy Act. This means that acts and practices of APP entities that are exempt from the Privacy Act will also be exempt from the NDB scheme.

For example, in some circumstances, private sector employers do not have to comply with the APPs in relation to employee records associated with current and former employment relationships (s 7B(3)). If an exempt employee record is subject to unauthorised access, disclosure

---

11 'Personal information' is defined in s 6(1) of the Privacy Act to include information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

12 See www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/businesses/small-business#what-does-trading-in-personal-information-mean.

13 Available online at www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/health-service-providers/is-my-organisation-a-health-service-provider.

14 Available online at www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#app-entity.

or loss, the private sector employer does not have to assess the breach or notify individuals and the Commissioner. This exemption does not apply to TFN information that is contained within an employee record. However, given community expectations around the handling of their personal information, it is recommended that employers notify affected individuals where a breach of an employee record is likely to result in serious harm. Doing so will enable affected individuals to take protective action against any potential harms, as well as illustrating to employees that the security of their records is taken seriously.

Further information about acts and practices that are exempt from the APPs and, by extension, the NDB scheme can be found in *Privacy business resource 13: Application of the Australian Privacy Principles to the private sector*.[15]

Small business operators

A small business operator (SBO) is an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than $3 million in any financial year since 2001 (s 6D).

Generally, SBOs do not have obligations under the APPs unless an exception applies (s 6D(4)).

In certain circumstances an SBO must comply with the APPs, and therefore with the NDB scheme. That will be the case where the SBO

- holds health information and provides a health service
- is related to an APP entity
- trades in personal information. That is, the SBO discloses personal information about individuals to anyone else for a benefit, service or advantage; or provides a benefit, service or advantage through the collection of personal information about another individual from anyone else
- is a credit reporting bodies
- is an employee associations registered under the *Fair Work (Registered Organisations) Act 2009*
- has 'opted-in' to APP coverage under s 6EA of the Privacy Act.

If an SBO carries on certain activities it must comply with the APPs, and therefore must comply with the NDB scheme, but only in relation to personal information held by the entity for the purpose of, or in connection with, those activities. Those activities include:

- providing services to the Commonwealth under a contract
- operating a residential tenancy data base
- reporting under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- conducting a protected action ballot
- information retained under the mandatory data retention scheme, as per Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*.

[15] Available online at www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-13.

More information about how to determine whether a business or organisation is an APP entity or subject to the APPs for some of its activities is available at *Privacy business resource 10: Does my small business need to comply with the Privacy Act?*.[16]

Credit reporting bodies

A credit reporting body (CRB) is a business or undertaking that involves collecting, holding, using, or disclosing personal information about individuals for the purpose of providing an entity with information about the credit worthiness of an individual (s 6P). Credit reporting information is defined as credit information or CRB derived information about an individual (s 6(1)).

CRBs have obligations under the NDB scheme in relation to their handling of credit reporting information (s 26WE(1)(b)), and in relation to their handling of any other personal information for which they have obligations under APP 11.

Credit providers

The NDB scheme applies to all credit providers whether or not they are APP entities. The section of the Privacy Act under which a credit provider is required to comply with the scheme will depend on what kind of information is involved in the data breach.

If it is 'credit eligibility information' (defined in s 6(1)) the NDB scheme will apply because of the security requirement in s 21S(1) in relation to that information.

If the credit provider is also an APP entity the NDB scheme applies in relation to other personal information because of the security requirement in APP 11.

The organisations that are credit providers for the purposes of the Privacy Act (s 6G) are:

- a bank
- an organisation or small business operator if a substantial part of its business is the provision of credit, such as a building society, finance company or a credit union
- a retailer that issues credit cards in connection with the sale of goods or services
- an organisation or SBO that supplies goods and services where payment is deferred for seven days or more, such as telecommunications carriers, and energy and water utilities
- certain organisations or SBOs that provide credit in connection with the hiring, leasing, or renting of goods.

An organisation or SBO that acquires the right of a credit provider in relation to the repayment of an amount of credit is also considered a credit provider, but only in relation to that particular credit (s 6K).

For more information about categories of credit-related personal information, see *Privacy business resource 3: Credit reporting – what has changed.*[17]

---

[16] Available online at www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10.

[17] Available online at www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-3-credit-reporting-what-has-changed.

TFN recipients

The NDB scheme applies to TFN recipients[18] in relation to their handling of TFN information (s 26WE(1)(d)). A TFN recipient is any person who is in possession or control of a record that contains TFN information (s 11). TFN information is information that connects a TFN with the identity of a particular individual (s 6).

A TFN recipient may also be an APP entity or credit provider. In certain circumstances, entities that are not otherwise covered by the Privacy Act, such as state and local government bodies, may also be authorised to receive TFN information and will be considered TFN recipients.

The NDB scheme applies to TFN recipients to the extent that TFN information is involved in a data breach. If TFN information is not involved, a TFN recipient would only need to comply with the NDB scheme for breaches of other types of information if they are also a credit provider or APP entity.

More information about TFN recipients is available in *Privacy business resource 12: The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information*.[19]

Overseas activities

Entities with an 'Australian link'

The NDB scheme generally extends to the overseas activities of an Australian Government agency (s 5B(1)). It also applies to organisations (including small businesses covered by the Act, outlined above) that have an 'Australian link' (s 5B(2)).

An organisation has an Australian link either because it is, in summary, incorporated or formed in Australia (see s 5B(1A) for more detail), or where:

- it carries on business in Australia or an external Territory, and
- it collected or held personal information in Australia or an external Australian Territory, either before or at the time of the act or practice (s 5B(3)).

Further information about entities that are taken to have an Australian link is available in Chapter B of the *APP Guidelines*.[20]

Disclosing personal information overseas

If an APP entity discloses personal information to an overseas recipient, in line with the requirements of APP 8.1, then the APP entity is deemed to 'hold' the information for the purposes of the NDB scheme (s 26WC(1)). APP 8.1 says that an APP entity that discloses personal information to an overseas recipient is required to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. This means that if the personal information held by the overseas recipient is subject to loss, unauthorised access, or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the

---

[18] Referred to in the Privacy Act and *Privacy (Tax File Number) Rule 2015* as 'file number recipients'.

[19] Available online at www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-12-the-privacy-tax-file-number-rule-2015-and-the-protection-of-tax-file-number-information.

[20] Available online at www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#australian-link.

Privacy Act, and if it is, for notifying individuals at risk of serious harm and providing a statement to the Commissioner.

There are exceptions to the requirement in APP 8.1 to take reasonable steps. APP entities that disclose information overseas under an exception in APP 8.2 are not taken to 'hold' information they have disclosed overseas under s 26WC. In these circumstances, if the personal information held by the overseas recipient is subject to a data breach, the APP entity does not have obligations to notify about the breach under the NDB scheme.

More information about APP 8 is available in *Privacy business resource 8: Sending personal information overseas*.[21]

Disclosing credit eligibility information

If a credit provider discloses credit eligibility information about one or more individuals to a person, a body or a related body corporate that does not have an 'Australian link' (s 26WC(2)(a)),[22] the credit provider may also have obligations under the NDB scheme in respect of that information. In the event that credit eligibility information held by the person or related body corporate is subject to loss, unauthorised access, or disclosure, the credit provider is responsible for assessing whether there is an eligible data breach that needs to be notified to individuals at risk of serious harm and the Commissioner.

[21] Available online at www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-8.

[22] This section only applies to a disclosure of credit eligibility information by a credit provider to a related body corporate under s 21G(3)(b), to a person processing an application for credit made to the credit provider or to a person who manages credit provided by the credit provider under s 21G(3) or to a debt collector under s 21M(1) of the Privacy Act.

Data breaches involving more than one entity

Key points

- The NDB scheme recognises that entities often hold personal information jointly. For example, one entity may have physical possession of the information, while another has legal control or ownership.
- In these circumstances, an eligible data breach of one entity will also be considered an eligible data breach of other entities that hold the affected information. Both will have obligations under the NDB scheme.
- In general, compliance by one entity will also be taken as compliance by each of the entities that hold the information. As such, only one entity needs to take the steps required by the NDB scheme. The NDB scheme leaves it up to the entities to decide which of them should do so.
- OAIC suggests that, in general, the entity with the most direct relationship with the individuals affected by the data breach should carry out notification.

When is information held jointly?

Under s 6(1) of the Privacy Act, an entity is taken to 'hold' personal information if it has possession or control of a record that contains personal information. This means that the term 'holds' extends beyond physical possession of a record to include a record that an entity has a right or power to deal with, even if it does not physically possess the record or own the medium on which it is stored.

For example, one entity may store its records with a cloud service provider. Since the cloud service provider has possession of the records, it will be taken to hold the personal information. Because the first entity has contractual rights to retain control of the records (such as maintaining rights to access and use the records), both entities hold the information.

Whether an entity will be taken to 'hold' personal information will therefore depend on the particular circumstances of the arrangement.

Other examples where two or more entities may hold the same information include:

- outsourcing arrangements
- Commonwealth contracts
- joint ventures.

Example
A large market research company is conducting focus groups on behalf of its client, a fast food outlet, using a list of interviewees provided by its client for that purpose. The contractual arrangements between the market research company and the fast food outlet give the fast food outlet effective control over how the information is handled by the research company. Following the focus group sessions, all participants give consent to participate in future research projects for the research company's other clients. The research company creates a new record containing the participant's names and contact details.

Although the record contains the same information that the market research company originally received from the fast food outlet, only the market research company has possession or control over the newly created record. This means that only the market research company would have NDB scheme obligations in the event of a data breach affecting the newly created record.

Responding to data breaches of jointly held information

In situations where two or more entities hold the same record of personal information, both entities are generally responsible for complying with the NDB scheme in relation to this record.

However, exceptions apply so that only one of the entities that jointly holds information needs to comply with the NDB scheme's assessment and notification requirements on behalf of the group. For example, if a data breach affects one or more other entities that jointly hold personal information, and one entity has assessed the suspected breach, the other entities are not required to also assess the breach (s 26WJ). If no assessment is conducted, depending on the circumstances, each entity that holds the information may be found to be in breach of the assessment requirements.

Similarly, only one entity needs to notify individuals and the Commissioner (s 26WM) if there is an eligible data breach involving personal information jointly held by more than one entity (see *Identifying eligible data breaches*). If none of the entities notify, then all of the entities may be found to have breached the notification requirements of the NDB scheme (s 26WL(2)).

See *Exceptions to notification obligations* for more information about the circumstances in which specific exceptions apply to entities that jointly hold information.

How to allocate responsibility for compliance

Each entity that holds personal information involved in an eligible data breach, should be able to demonstrate they are meeting the requirements of the NDB scheme.

The NDB scheme does not prescribe which entity should conduct an assessment of a suspected data breach, nor which entity should notify individuals and the Commissioner about an eligible data breach. This allows entities to tailor their arrangements to accommodate their particular contractual and customer relationships.

Accordingly, where information is held jointly, entities should establish clear procedures for complying with the NDB scheme when entering into service agreements or other relevant contractual arrangements. This may include considering obligations around the communication of suspected breaches, processes for conducting assessments, and responsibility for containment, remediation, and notification.

The Commissioner suggests that, in general, the entity with the most direct relationship with the individuals at risk of serious harm may be best placed to notify. This will allow individuals to better understand the notification, and how the eligible data breach might affect them.

Example

A medical practice stores paper-based patient records with a contracted storage provider. The storage provider's premises are broken into and a number of items stolen. While the storage provider cannot immediately determine if the stolen items included the medical practice's records, it suspects that they might have been included. Both the medical practice and the storage provider hold the records for the purpose of the Privacy Act, so both have an obligation to conduct an assessment and, if required, notify.

Since the storage provider is more familiar with its facilities, the entities decide that the storage provider is best placed to conduct an assessment and determine if the records were stolen. Once the provider determines that the records were stolen, the medical practice assists the assessment by using its knowledge about the affected individuals to conclude that serious harm is likely. Although the storage provider's insurance company has agreed to cover the cost of notification, the storage provider and medical practice agree that it is most appropriate that notification come from the medical practice, as the relevant individuals do not have any pre-existing relationship with the storage provider. As such, the medical practice notifies the individuals about the incident and is reimbursed by the storage provider and its insurer for the costs of notification.

Identifying eligible data breaches

Key points

- The NDB scheme requires regulated entities to notify particular individuals and the Commissioner about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.
- Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position.
- Not all data breaches are eligible. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the Commissioner. There are also exceptions to notifying in certain circumstances.

Eligible data breach

An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds (see, *What is a 'data breach'?*)
2. this is likely to result in serious harm to one or more individuals (see, *Is serious harm likely?*), and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action (see *Preventing serious harm with remedial action*).

This document is about the threshold at which an incident is considered an 'eligible data breach' that will be notifiable under the scheme unless an exception applies. *Assessing a suspected data breach* provides guidance to entities about the process to follow when carrying out an assessment of 'whether there are reasonable grounds to suspect that there may have been an eligible data breach of the entity' under s 26WH.

What is a 'data breach'?

The first step in deciding whether an eligible data breach has occurred involves considering whether there has been a data breach; that is, unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information (s 26WE(2)). The Privacy Act does not define these terms. The following analysis and examples draw on the ordinary meaning of these words.

- ***Unauthorised access*** of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

  Examples of unauthorised access include:

  - an employee browsing sensitive customer records without any legitimate purpose

- a computer network being compromised by an external attacker resulting in personal information being accessed without authority.

- ***Unauthorised disclosure*** occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.

  For example, an employee of an entity accidentally publishing a confidential data file containing the personal information of one or more individuals on the internet would be considered unauthorised disclosure

- ***Loss*** refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure.

  An example is where an employee of an entity leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport. Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach (s 26WE(2)(b)(ii)). For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach.

Is serious harm likely?

The second step in deciding whether an eligible data breach has occurred involves deciding whether, from the perspective of a reasonable person, the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach.

For the NDB scheme a 'reasonable person' means a person in the entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach. In general, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach. 'Reasonable person' is also discussed in general terms in Chapter B of the OAIC's *APP Guidelines*.[23]

The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible).

'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

Entities should assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm. The NDB scheme includes a non-exhaustive list of 'relevant matters'

[23] Available online at www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#reasonable-reasonably.

that may assist entities to assess the likelihood of serious harm. These are set out in s 26WG as follows:

- the kind or kinds of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security technology or methodology:
  - was used in relation to the information, and;
  - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information
- the likelihood that the persons, or the kinds of persons, who:
  - have obtained, or who could obtain, the information, and;
  - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;
  - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters.

As some of these matters involve overlapping considerations, they are discussed further below, under the broader headings:

1. the type or types of personal information involved in the data breach
2. the circumstances of the data breach
3. the nature of the harm that may result from the data breach.

The type or types of personal information involved in the data breach

Some kinds of personal information may be more likely to cause an individual serious harm if compromised. Examples of the kinds of information that may increase the risk of serious harm if there is a data breach include:

- 'sensitive information',[24] such as information about an individual's health
- documents commonly used for identity fraud (including Medicare card, driver licence, and passport details)
- financial information

[24] See s 6(1) of the Privacy Act for categories of personal information that are covered by the definition of 'sensitive information'.

- a combination of types of personal information (rather than a single piece of personal information) that allows more to be known about the individuals the information is about.

Circumstances of the data breach

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual. This may include consideration of the following:

- **Whose personal information was involved in the breach?** An entity could consider whose personal information was involved in the breach, as certain people may be at particular risk of serious harm. A data breach involving the names and addresses of individuals might not, in various circumstances, be likely to result in serious harm to an individual, particularly if that information is already publicly available. However, if the entity knows that the information involved primarily relates to individuals known to be vulnerable, this may increase the risk of serious harm

- **How many individuals were involved?** If the breach involves the personal information of many individuals, the scale of the breach should affect an entity's assessment of likely risks. Even if an entity considers that each individual will only have a small chance of suffering serious harm, if more people's personal information is involved in the breach, it may be more likely that at least some of the individuals will experience serious harm. From a risk perspective, it may be prudent, depending on the particular circumstances, to assume a breach involving the personal information of a very large number of people is likely to result in serious harm to at least one of those individuals, unless context or circumstances would support this not being the case

- **Do the circumstances of the data breach affect the sensitivity of the personal information?** A breach that may publicly associate an individual's personal information with a sensitive product or service they have used may increase the risk of serious harm. For example, a data breach involving an individual's name may involve a risk of serious harm if the entity's name links the individual with a particular form of physical or mental health care[25]

- **How long has the information been accessible?** The time between when the data breach occurred and when the entity discovers the breach will be relevant to the entity's consideration of whether serious harm is likely to occur. For example, if personal information is publically accessible for a significant period before the entity is aware of the data breach, it may be more likely that the personal information have been accessed in ways that will result in serious harm to the individuals affected

- **Is the personal information adequately encrypted, anonymised, or otherwise not easily accessible?** A relevant consideration is whether the information is rendered unreadable through the use of security measures to protect the stored information, or if it is stored in such a way so that it cannot be used if breached. In considering whether security measures (such as encryption) applied to compromised data are adequate, the entity should consider whether the method of encryption is an industry-recognised secure standard at the time the entity is assessing the likelihood of risk. Additionally, an entity should have regard to whether the unauthorised recipients of the personal information would have the capability to circumvent

[25] Another example would include the information disclosed in the Ashely Madison data breach in 2015. See www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison.

these safeguards. For example, if an attacker holds both encrypted data and the encryption key needed to decrypt that data, the entity should not assume the data is secure

- **What parties have gained or may gain unauthorised access to the personal information?** The unauthorised disclosure of an individual's criminal record to someone who knows that individual personally may increase the risk of serious reputational harm for that individual. In addition, where a third party that obtains unauthorised access to personal information, or appears to target personal information of a particular individual or group of individuals, this may increase the risk of serious harm as it may be more likely the personal information is intended for malicious purposes.

The nature of the harm

In assessing the risk of serious harm, entities should consider the broad range of potential kinds of harms that may follow a data breach. It may be helpful for entities assessing the likelihood of harm to consider a number of scenarios that would result in serious harm and the likelihood of each. Examples may include:

- identity theft
- significant financial loss by the individual
- threats to an individual's physical safety
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

Preventing serious harm with remedial action

The NDB scheme provides entities with the opportunity to take positive steps to address a data breach in a timely manner, and avoid the need to notify. If an entity takes remedial action such that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach for that entity or for any other entity (s 26WF(1), s 26WF(2), s 26WF(3)). For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information (s 26WF(3)).

If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

Examples of remedial action that may prevent serious harm occurring include:

Example 1

A data file, which includes the personal information of numerous individuals, is sent to an incorrect recipient outside the entity. The sender realises the error and contacts the recipient, who advises that the data file has not been accessed. The recipient has an ongoing contractual relationship with the sender, and regards the recipient as reliable and trustworthy. The sender then confirms that the recipient has not copied, and has permanently deleted the data file. In the circumstances, the sender decides that there is no likely risk of serious harm.

Example 2

An employee leaves a smartphone on public transport while on their way to work. When the employee arrives at work they realise that the smartphone has been lost, and ask their employer's IT support staff to remotely delete the information on the smartphone. Because of the security measures on the smartphone, the IT support staff are confident that its content could not have been accessed in the short period between when it was lost and when its contents were deleted.

Examples of data breaches

The following examples are provided to illustrate some of the considerations that entities might take into account when assessing whether a data breach is likely to result in serious harm. However, whether any data breach is notifiable depends on the particular circumstances of the breach.

The acts and practices described in these examples may raise other issues under the Privacy Act, such as whether these organisations have taken reasonable steps to secure personal information, as required by APP 11.1.

Example 1 — strong encryption making notification unnecessary

Insure, an insurance company, decides to update its customer relationship management and record keeping software. While running a test, the IT team installing the software discovers that some customer records were accessed by an unauthorised third party more than a year ago. The customer records involved are primarily encrypted payment card information.

Since *Insure* suspects fraudulent activity as the motive for the unauthorised access, it notifies the police and hires an external IT security consultant to conduct an audit and security assessment. The audit confirms that 500 customer records were involved in the data breach, and that an overseas source was responsible for the hack. The IT security consultant's comprehensive sweeps of the internet and dark web were unable to find evidence that the information was

offered for sale or otherwise disclosed online. The IT security consultant also assesses that because of the high standard of encryption used for the credit card information, it is unlikely that this information could be accessed by the hacker. Insure implemented the recommendations of its IT security consultant, including new IT security protocols and intrusion detection software.

Insure determines that it is not likely that the individuals whose personal information is involved in the data breach are at risk of serious harm. Therefore, *Insure* decides it is not an eligible data breach, and is not required to notify affected individuals or the Commissioner.

Nonetheless, it decides that as a customer service measure, it should tell the individuals about the incident. It sends an email to the customers informing them of the incident and providing some advice on personal information security measures they can take. This notification is not required by the NDB scheme, so can take any form that *Insure* considers appropriate.

Example 2 — notification following unintentional publication of sensitive data

Medicines, a chain of low-cost pharmacies, becomes aware that its customer database, including records about dispensing of prescription drugs, has been publicly available on the internet due to a technical error. *Medicines'* security consultants identify that the database was publicly available for a limited time and that it was only accessed a few times.

However, *Medicines* is unable to determine who accessed the data or if they kept a copy. Given the sensitivity of the personal information contained in the database, including drugs related to the treatment of addictive and psychiatric conditions, *Medicines'* risk assessment concludes that the data breach would be likely to result in serious harm to some of its customers.

Medicines decides to notify all customers whose personal information is involved in the data breach and the Commissioner. Because it does not have contact details for many of the customers who filled prescriptions with it in person, it publishes a notice describing the breach on its website and posts a copy in a prominent location at each of its stores.

Example 3 — data breach experienced by overseas contractor leading to phishing

Consumestuff enters into a contract with an automated email marketing platform located overseas, which it uses to communicate with its customers. The service provider detects that the bulk mailing distribution lists for *Consumestuff* have been downloaded by an external IP address. The bulk mailing distribution lists include the name, email address, gender, and suburb of *Consumestuffs'* customers. The service provider notifies *Consumestuff*, who conducts an immediate investigation into how the mailing lists were accessed and downloaded.

An IT security sweep detects malware on a *Consumestuff* employee's computer, and the investigation concludes that the employee's login credentials for the service provider were

obtained after the employee unintentionally opened an email attachment from a malicious third party attacker. As *Consumestuff* also held the personal information, and assuming that the service provider is not an APP entity, *Consumestuff* undertakes an assessment to determine whether it is required to notify individuals and the Commissioner.

As part of its assessment, *Consumestuff* identifies that some of the individuals whose personal information was involved in the data breach received emails that fraudulently claimed to be sent from *Consumestuff* asking for customer credit card details. Given this information, *Consumestuff* concludes that it is more probable than not that the attacker will use the information in the mailing lists for the purposes of fraud or identity theft, and that it is likely that some of the individuals will suffer serious financial harm as a result of this.

Given this likelihood, *Consumestuff* sends an email with the relevant information required by the NDB scheme to those individuals whose personal information is involved in the data breach, and notifies the Commissioner. *Consumestuffs'* email to these individuals includes information about scam emails and how to identify them, and provides referrals to services that assist individuals in mitigating the risk of identity theft.

Example 4 — loss of unencrypted storage media containing personal information

A member of the human resources team of a Government Department (the Department) copies the employee records of the Department's 2000 employees onto a portable memory stick, to do work at home. This action was in breach of the Department's policies, and Australian Privacy Principle 11. The memory stick is lost by the employee who held it. They report this to their manager.

The Department follows its data breach response plan, and as a first step conducts a search for the memory stick, but fails to locate it. The information contained in the memory stick includes the names, salary information, TFNs, home addresses, phone numbers, birth dates, and in some cases health information (including disability information) of current staff. As the data on the memory stick is not encrypted, the Department concludes that unauthorised access is likely to occur.

Due to the sensitivity of the unencrypted information – not only the extent and variety of the information, but also the inclusion of health and disability information in the records – the Department's risk assessment finds that there is a likely risk of serious harm to at least one of the individuals whose personal information is involved in the data breach. On this basis, the Department considers that it is an eligible data breach for the purposes of the NDB scheme, and prepares a statement to notify the Commissioner.

A senior staff member emails the relevant staff to notify them of the eligible data breach, and provides the content of the statement prepared for the Commissioner. In the notification, the Department also offers staff an apology for the breach, notes that the OAIC has been informed of the breach, and explains what steps have been put in place to prevent this type of a breach occurring in the future.

Example 5 — online banking fraud and remedial action

A bank's fraud detection systems flag that there has been unusual activity on an individual's online banking account, when a substantial amount of money is transferred to an account in another country. The fraud team assesses the activity, and finds that the account was accessed by an unauthorised attacker who had obtained control of the individual's account.

Through its existing fraud management processes, the bank's fraud team notify the individual that it is temporarily freezing online access to the account due to the fraudulent activity, resets the password for online access and returns the stolen funds. As part of its risk assessment, the fraud team confirms that the individual's other accounts have not been compromised, and recommends to the individual that they change any similar passwords to other services. A member of the bank's fraud team assesses whether there is a risk of likely harm to the individual, and concludes that as a result of the above steps taken to remediate the unauthorised access, it is not likely the individual will be at risk of serious harm. Given this remedial action, the bank does not notify the Commissioner.

Example 6 — email sent to the wrong recipient contained before serious harm can occur

CareHeeps, a claims management service provider, regularly sends updates to its clients about the status of the workers compensation claims of their employees. Because of human error, an employee of *CareHeeps* accidentally sends an email with an attachment about the employees of Business A to another client, Business B. The attachment contains the personal information of 200 employees of Business A, and includes their name, address, date of birth, and health information about their claimed injury.

A *CareHeeps* employee realises the error, and contacts Business B to delete the email with the attachment. Business B confirms that one of its employees accessed the file without initially realising the error, but provides written confirmation that it has since deleted all copies of the email and attachment. The employee who accessed the file has also undertaken not to divulge the information. *CareHeeps'* assessment of the remedial action taken concludes that, while the file included sensitive information about the individuals' health, its contractual arrangements with Business B and the written assurance provided by Business B has prevented the likely risk of serious harm to any individuals. As a consequence, *CareHeeps* determines that it is not an eligible data breach that needs to be notified to individuals or the Commissioner.

Exceptions to notification obligations

Key points

- The NDB scheme requires regulated entities to notify individuals and the Commissioner of 'eligible data breaches'. A data breach is an eligible data breach if an individual is likely to experience serious harm (see *Identifying eligible data breaches* and *Notifying individuals about an eligible data breach*).
- There are some exceptions to the notification requirements, which relate to:
  - eligible data breaches of other entities (see *Data breaches involving more than one entity*)
  - enforcement related activities
  - inconsistency with secrecy provisions
  - declarations by the Commissioner.
- Data breaches that are notified under s 75 of the My Health Records Act, do not need to be notified under the NDB scheme.

Enforcement related activities

An enforcement body does not need to notify individuals about an eligible data breach if its chief executive officer (CEO) believes on reasonable grounds that notifying individuals would be likely to prejudice an enforcement related activity conducted by, or on behalf, of the enforcement body (s 26WN).[26]

'Believes on reasonable grounds' means the CEO must have a basis for the belief. It is the responsibility of the enforcement body to be able to justify the reasonable grounds for this belief, and the decision should be documented. 'Reasonable belief' is discussed further in Chapter B of the OAIC's APP Guidelines.[27]

The enforcement body must still provide a statement about the eligible data breach to the Commissioner (see *What to include in an eligible data breach statement*). However, this statement does not have to include the steps recommended for individuals to take in response to the data breach, because individuals are not being notified (s 26WN).

If this exception applies, and the eligible data breach involves other entities, these other entities are not required to notify individuals (s 26WN(e)). Further, these other entities are not required to provide a statement about the eligible data breach to the Commissioner if the enforcement body has done so (s 26WM). To rely on this exception, other entities would usually need a written statement regarding the eligible data breach, dated and signed by the CEO of the enforcement body.

This exception does not apply if an eligible data breach is unrelated to an enforcement activity. For example, the exception may not apply to an eligible data breach involving employees' personal information, which is unrelated to an investigation.

---

[26] See s 6(1) of the Privacy Act for definitions of enforcement body and enforcement related activity.

[27] Paragraphs B.110-B.111.

Inconsistency with secrecy provisions

Exceptions to notifying individuals or the Commissioner may apply where a Commonwealth law prohibits or regulates the use or disclosure of information (a secrecy provision). In particular:

- the requirement to provide a statement to the Commissioner about the eligible data breach does not apply to the extent that this requirement is inconsistent with a secrecy provision (s 26WP(2))
- the requirement to notify individuals about an eligible data breach does not apply to the extent that providing this notice is inconsistent with a secrecy provision (s 26WP(3)).

The exceptions in s 26WP are intended to preserve the operation of specific secrecy provisions in other legislation. A common purpose of secrecy provisions is to prohibit the unauthorised disclosure of client information. Most secrecy provisions allow the disclosure of information in certain circumstances, such as with an individual's consent where the information relates to them, or where the disclosure of information relates to an officer's duties, or the exercise of their powers or functions.

If an eligible data breach occurs, agencies should apply the exceptions under s 26WP only to the extent necessary to avoid inconsistency with a secrecy provision.

For example, if providing a statement about an eligible data breach to the Commissioner (s 26WK) would not be inconsistent with a secrecy provision, but notifying individuals (s 26WL) would be, the entity would only be required to notify the Commissioner.

The following is relevant in assessing whether a secrecy provision is inconsistent with the requirements of the NDB scheme:

- If a secrecy provision permits the disclosure of information that is required or authorised by another law (such as the Privacy Act), there would not be an inconsistency between the secrecy provision and the NDB scheme notification requirements.
- If a secrecy provision does not allow the disclosure of information, even if the disclosure is required or authorised by another law (such as the Privacy Act), there may be inconsistency between the secrecy provision and the NDB scheme notification requirements.
- If a secrecy provision permits the disclosure of information in the course of an officer's duties, there would not be inconsistency between the secrecy provision and the NDB scheme notification requirements, as complying with the notification requirements is the responsibility of the agency through its officers.

Declarations by the Australian Information Commissioner

In some circumstances, the Commissioner may declare by written notice that an entity does not need to comply with the NDB scheme notification requirements (s 26WQ) in relation to a specific eligible data breach. The purpose of the declaration by the Commissioner is to provide an exception where compliance with the NDB notification requirements would conflict with the public interest.

The Commissioner may declare that an entity is not required to provide a statement to the Commissioner or to notify particular individuals (s 26WQ(1)(c)), or that notification to individuals is delayed for a specified period (s 26WQ(1)(d)).

The Commissioner cannot make a declaration under s 26WQ unless satisfied that it is reasonable in the circumstances to do so, having regard to the public interest, relevant advice received from an enforcement body or the Australian Signals Directorate, and any other relevant matter. While the Commissioner is empowered to make a declaration if it is 'reasonable in the circumstances to do so', the Commissioner still has discretion about whether to make a declaration, and on what terms.

In deciding whether to make a declaration, and on what terms, the Commissioner will have regard to the Objects of the Privacy Act and other relevant matters. The Commissioner will consider whether the risks associated with notifying of a particular eligible data breach outweigh the benefits of notification to individuals at risk of serious harm.

Given the clear objective of the scheme to promote notification of eligible data breaches, and the inclusion of exceptions in the scheme that remove the need to notify in a wide range of circumstances, the Commissioner expects that declarations under s 26WQ will only be made in exceptional cases and only after a compelling case has been put forward by the entity seeking the declaration.

The procedure for applying for a declaration, and factors the Commissioner may consider, are outlined in the OAIC's *Guide to OAIC Privacy Regulatory Action — Chapter 9: Data breach incidents (draft).*

My Health Record system data breaches

Certain participants in the My Health Record system (such as the System Operator, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider), are required to report data breaches that occur in relation to the My Health Record system to the either the System Operator or the Commissioner, or both, depending on the entity reporting the data breach (s 75 of the My Health Records Act). If a data breach has been, or is required to be, notified under s 75 of the My Health Records Act, the NDB scheme does not apply (s 26WD). This exception is intended to avoid duplication of notices under the NDB scheme and the data breach notification requirements in the My Health Record system.

Information about data breach notification requirements of the My Health Records Act is available in the OAIC's *Guide to mandatory data breach notification in the My Health Record system*.[28]

Only notifications under s 75 of the My Health Records Act fall within this exception. Notifications under other schemes such as that within the National Cancer Screening Register Act are not excluded from the NDB scheme.

[28] Available online at www.oaic.gov.au/agencies-and-organisations/guides/guide-to-mandatory-data-breach-notification-in-the-my-health-record-system.

Example

A practice manager who has access to the My Health Record system for administrative purposes only, accesses a patient's My Health Record clinical information without authorisation. The GP discovers this incident and immediately notifies the System Operator and the Commissioner as required under s 75 of the My Health Records Act. There is no need to also notify this data breach under the Privacy Act.

At or about the same time, the practice manager also accesses the GP's clinical database (not part of the My Health Record system), and downloads their ex-partner's health information without authorisation. Upon discovering this incident, the GP takes immediate steps to contain the breach and, due to the nature of the relationship between the practice manager and the patient, decides there is a likelihood of serious harm to the patient in the circumstances. The GP notifies the patient and the Commissioner about the data breach, as required under the Privacy Act's NDB scheme.

Assessing a suspected data breach

Key points

- If an entity has reasonable grounds to *believe that it has* experienced an eligible data breach, it must promptly notify individuals and the Commissioner about the breach, unless an exception applies.
- In contrast, if an entity *suspects that it may* have experienced an eligible data breach, it must quickly assess the situation to decide whether or not there has been an eligible data breach.
- An assessment must be reasonable and expeditious, and entities may develop their own procedures for assessing a suspected data breach.

When must entities assess a suspected breach?

The NDB scheme is designed so that only serious ('eligible') data breaches are notified (see *Identifying eligible data breaches*). If an entity is aware of reasonable grounds to *believe that there has been* an eligible data breach, it must promptly notify individuals at risk of serious harm and the Commissioner about the eligible data breach (see *Notifying individuals about an eligible data breach*).

On the other hand, if an entity only has reason to *suspect that there may have been* a serious breach, it needs to move quickly to resolve that suspicion by assessing whether an eligible data breach has occurred. If, during the course of an assessment, it becomes clear that there has been an eligible breach, then the entity needs to promptly comply with the notification requirements.

The requirement for an assessment is triggered if an entity is aware that there are reasonable grounds to suspect that there may have been a serious breach (s 26WH(1)).

Whether an entity is 'aware' of a suspected breach is a factual matter in each case, having regard to how a reasonable person who is properly informed would be expected to act in the circumstances. For instance, if a person responsible for compliance or personnel with appropriate seniority are aware of information that suggests a suspected breach may have occurred, an assessment should be done. An entity should not unreasonably delay an assessment of a suspected eligible breach, for instance by waiting until its CEO or board is aware of information that would otherwise trigger reasonable suspicion of a breach within the entity.

The Commissioner expects entities to have practices, procedures, and systems in place to comply with their information security obligations under APP 11, enabling suspected breaches to be promptly identified, reported to relevant personnel, and assessed if necessary.

How quickly must an assessment be done?

An entity must take all reasonable steps to complete the assessment within **30 calendar days** after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach (s 26WH(2)).

The Commissioner expects that wherever possible entities treat 30 days as a maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.

Where an entity cannot reasonably complete an assessment within 30 days, the Commissioner recommends that it should document this, so that it is able demonstrate:

- that all reasonable steps have been taken to complete the assessment within 30 days
- the reasons for the delay
- that the assessment was reasonable and expeditious.

How is an assessment done?

Entities must carry out a 'reasonable and expeditious' assessment (s 26WH(2)(a)). The Privacy Act does not set out how entities should assess a data breach, and entities may develop their own procedures for assessing a suspected breach.

The Commissioner expects that the amount of time and effort entities will expend in an assessment should be proportionate to the likelihood of the breach and its apparent severity.

The Commissioner expects that an entity's approach to data breach management, including its data breach response plan, will incorporate the requirements of the NDB scheme for assessing suspected eligible data breaches.

While the Privacy Act does not specify how an assessment should occur, the OAIC suggests that an assessment could be a three-stage process:

1. **Initiate:** decide whether an assessment is necessary and identify which person or group will be responsible for completing it
2. **Investigate:** quickly gather relevant information about the suspected breach including, for example, what personal information is affected, who may have had access to the information and the likely impacts
3. **Evaluate**: make a decision, based on the investigation, about whether the identified breach is an eligible data breach (see *Identifying eligible data breaches*).

The Commissioner recommends that entities document the assessment process and outcome.

Remedial action

At any time, including during an assessment, an entity can, and should, take steps to reduce any potential harm to individuals caused by a suspected or eligible data breach. If remedial action is successful in preventing serious harm to affected individuals, notification is not required (as explained in *Identifying eligible data breaches*).

Breach established — what next?

Once an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach – whether during the course of an assessment, or when the assessment is complete – it must promptly notify affected individuals and the Commissioner about the breach (see *What to include in an eligible data breach statement* and *Notifying individuals about an eligible data breach*).

Notifying individuals about an eligible data breach

Key points

- When an entity experiences a data breach, its first step should be to contain the breach where possible and take remedial action. Where serious harm cannot be mitigated through remedial action (see *Identifying eligible data breaches*), it must notify individuals at risk of serious harm and provide a statement to the Commissioner as soon as practicable.
- If it is not practicable to notify individuals at risk of serious harm, an entity must publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm.
- If a single eligible data breach applies to multiple entities, only one entity needs to notify the Commissioner and individuals at risk of serious harm. It is up to the entities to decide who notifies. Generally, the Commissioner suggests that the entity with the most direct relationship with the individuals at risk of serious harm should undertake the notification.

Who needs to be notified?

Once an entity has reasonable grounds to believe there has been an eligible data breach, the entity must, as soon as practicable, make a decision about which individuals to notify, prepare a statement for the Commissioner and notify individuals of the contents of this statement.

The NDB scheme provides flexibility — there are three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for the entity (s 26WL(2)).

Whether a particular option is practicable involves a consideration of the time, effort, and cost of notifying individuals at risk of serious harm in a particular manner. These factors should be considered in light of the capabilities and capacity of the entity.

Option 1 — Notify all individuals

If it is practicable, an entity can notify each of the individuals to whom the relevant information relates (s 26WL(2)(a)). That is, all individuals whose personal information was part of the eligible data breach.

This option may be appropriate, and the simplest method, if an entity cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but where the entity has formed the view that serious harm is likely for one or more of the individuals.

The benefits of this approach include ensuring that all individuals who may be at risk of serious harm are notified, and allowing them to consider whether they need to take any action in response to the eligible data breach.

Option 2 — Notify only those individuals at risk of serious harm

If it is practicable, an entity can notify only those individuals who are at risk of serious harm from the eligible data breach (s 26WL(2)(b)).

That is, individuals who are likely to experience serious harm as a result of the eligible data breach. If an entity identifies that only a particular individual, or a specific subset of individuals, involved in

an eligible data breach is at risk of serious harm, and can specifically identify those individuals, only those individuals need to be notified.

The benefits of this targeted approach include avoiding unnecessary distress to individuals who are not at risk, limiting possible notification fatigue among members of the public, and reducing administrative costs, where it is not required by the NDB scheme.

Example
An attacker installs malicious software on a retailer's website. The software allows the attacker to intercept payment card details when customers make purchases on the website. The attacker is also able to access basic account details for all customers who have an account on the website. Following a comprehensive risk assessment, the retailer considers that the individuals who made purchases during the period that the malicious software was active are at likely risk of serious harm, due to the likelihood of payment card fraud. Based on this assessment, the retailer also considers that those customers who only had basic account details accessed are not at likely risk of serious harm. The retailer is only required to notify those individuals that it considers to be at likely risk of serious harm.

Option 3 — Publish notification

If neither option 1 or 2 above are practicable, for example, if the entity does not have up-to-date contact details for individuals, then the entity must:

- publish a copy of the statement on its website if it has one
- take reasonable steps to publicise the contents of the statement (s 26WL(2)(c)).

It is not enough to simply upload a copy of the statement prepared for the Commissioner on any webpage of the entity's website. Entities must also take proactive steps to publicise the substance of the eligible data breach (and at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm.

While the Privacy Act does not specify the amount of time that an entity must keep the statement accessible on their website, the Commissioner would generally expect that it is available for at least 6 months.

Example
In the process of cleaning up his old desktop, an accountant accidently sends a spreadsheet containing the TFN and contact information of his past clients to his entire email contact list. He is worried that the information contained could be used for identity theft and understands that 'recalling' emails does not usually work. He emails his contact list to request that they immediately delete the spreadsheet and notify him when this has happened. In addition, since the file is over ten years old, he decides that notifying individuals directly (through option 1 or 2) would not be practicable, as their contact details

would more than likely be outdated. He notifies the Commissioner about the data breach and publicises a notification (option 3).

How do I notify and what do I need to say?

Options 1 (Notify all individuals) and 2 (Notify only those individuals at risk of serious harm)

Options 1 and 2 above require that entities take 'such steps as are reasonable in the circumstances to notify individuals about the contents of the statement' that the entity prepared for the Commissioner (s 26WL(2)(a) and (b)).

The entity can use any method to notify individuals (for example, a telephone call, SMS, physical mail, social media post, or in-person conversation), so long as the method is reasonable. In considering whether a particular method, or combination of methods is reasonable, the notifying entity should consider the likelihood that the people it is notifying will become aware of, and understand the notification, and weigh this against the resources involved in undertaking notification.

An entity can notify an individual using their usual method of communicating with that particular individual (s 26WL(4)). For example, if an entity usually communicates through a nominated intermediary, they may also choose to notify through this intermediary.

The entity can tailor the form of its notification to individuals, as long as it includes the content of the statement required by s 26WK. That statement (and consequently, the notification to individuals) must include the following information:

1. the identity and contact details of the entity (s 26WK(3)(a))
2. a description of the eligible data breach that the entity has reasonable grounds to believe has happened (s 26WK(3)(b))
3. the kind, or kinds, of information concerned (s 26WK(3)(c))
4. recommendations about the steps that individuals should take in response to the eligible data breach (s 26WK(3)(d)).

Decisions about the appropriate types of recommendations will always be dependent on the circumstances of the eligible data breach. This may include choosing to tailor recommended steps around an individual's personal circumstances, or providing general recommendations that apply to all individuals. In some circumstances, the entity may have already taken some protective steps, reducing the necessity for action by affected individuals. The entity may choose to explain these measures in the notice to individuals as a part of their recommendation. For example, a bank may notify an individual that it has suspended suspicious transactions on their account and recommended steps may be limited to suggesting the individual monitor their accounts and notify the bank immediately of any other suspicious transactions.

Option 3 (Publish notification)

Option 3, which can only be used if options 1 or 2 are not practicable, requires an entity to publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to publicise the contents of that statement.

An entity should consider what steps are reasonable in the circumstances of the entity and the data breach to publicise the statement. The purpose of publicising the statement is to draw it to the attention of individuals at risk of serious harm, so the entity should consider what mechanisms would be most likely to bring the statement to the attention of those people.

A reasonable step when publicising an online notice, might include:

- ensuring that the notice is prominently placed on the relevant webpage, which can be easily located by individuals and indexed by search engines
- publishing an announcement on the entity's social media channels
- taking out a print or online advertisement in a publication or on a website the entity considers reasonably likely to reach individuals at risk of serious harm.

In some cases, it might be reasonable to take more than one step to publicise the contents of the statement. For example, if a data breach involves a particularly serious form of harm, or affects a large number of individuals, an entity could take out multiple print or online advertisements (which could include paid advertisements on social media channels), publish posts on multiple social media channels, or use both traditional media and online channels.

The approach to publicising the statement may depend on the publication method. For example, where space and cost allows, an entity may republish the entirety of the information required to be included in the statement. Another option, if the available space is limited, or the cost of republishing the entire statement would not be reasonable in all the circumstances, would be to summarise the information required to be included in the statement and provide a hyperlink to the copy of the statement published on the entity's website. Entities should keep in mind the ability and likelihood of individuals at risk of serious harm being able to access the statement when determining the appropriateness of relying solely on such an approach.

If option 3 is chosen, entities should take care to ensure that the online notice does not contain any personal information. While it may help if entities provide a general description of the cohort of affected individuals, this description should not identify any of the affected individuals or provide information that may make an individual reasonably identifiable. For example, it may be appropriate for an online retailer to publicise that individuals who made transactions in the year 2013 may be affected, but it would not be appropriate for the retailer to publicise the names associated with any compromised transaction data.

Timing of notification

Entities must notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner (s 26WL(3)).

Considerations of cost, time, and effort may be relevant in an entity's decision about when to notify individuals. However, the Commissioner generally expects entities to expeditiously notify individuals at risk of serious harm about an eligible data breach unless cost, time, and effort are excessively prohibitive in all the circumstances.

If entities have notified individuals at risk of serious harm of the data breach before they notify the Commissioner, they do not need to notify those individuals again, so long as the individuals were notified of the contents of the statement given to the Commissioner. The scheme does not require that notification be given to the Commissioner before individuals at risk of serious harm, so if entities wish to begin notifying those individuals before, or at the same time as notifying the Commissioner, they may do so.

What to include in an eligible data breach statement

Key points

- The NDB scheme requires entities to notify individuals about an eligible data breach (see *Identifying eligible data breaches*).
- Entities are also required to prepare a statement and provide a copy to the Commissioner (s 26WK). The OAIC's online form may help entities to do this.
- The statement must include the name and contact details of the entity, a description of the eligible data breach, the kind or kinds of information involved, and what steps the entity recommends that individuals at risk of serious harm take in response to the eligible data breach (s 26WK(3))
- Entities must notify affected individuals about the contents of this statement or, if this is not practicable, publish a copy of the statement on the entity's website and take reasonable steps to publicise the contents of the statement (s 26WL(2)) (see Notifying individuals about an eligible data breach).

What must be included in the statement

A statement about an eligible data breach must include:

- the identity and contact details of the entity (s 26WK(3)(a))
- a description of the eligible data breach (s 26WK(3)(b))
- the kind or kinds of information involved in the eligible data breach (s 26WK(3)(c))
- what steps the entity recommends that individuals take in response to the eligible data breach (s 26WK(3)(d)).

Identity and contact details of the entity

Where an entity's company name is different to the business or trading name, the OAIC recommends that entities also include the name that is most familiar to individuals. The entity must also include information about how an individual can contact it. Depending on the nature and scale of the breach, the entity may wish to consider whether to provide its general contact details, or establish a dedicated phone line or email address to answer queries from individuals.

Description of the eligible data breach

An entity is required to include 'a description' of the data breach in its statement.

The OAIC expects that the statement will include sufficient information about the data breach to allow affected individuals the opportunity to properly assess the possible consequences of the data breach for them, and to take protective action in response.

Information describing the eligible data breach may include:

- the date, or date range, of the unauthorised access or disclosure
- the date the entity detected the data breach
- the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure)

- who has obtained or is likely to have obtained access to the information
- relevant information about the steps the entity has taken to contain or remediate the breach.

In general, the OAIC does not expect entities to identify the specific individuals who have accessed information, unless this is relevant to the steps the entity recommends individuals might take in response. For example, where information has been accidentally disclosed in a family violence situation known to the entity, this would be important information for the individual to know.

Usually, however, it would suffice to provide a general description of the type of person who has obtained the information, such as 'an external third party' or 'former employee'.

The kind or kinds of information concerned

The statement must include the kind or kinds of information involved in the data breach. Knowing what kind of personal information has been breached is critical to assessing what action should be taken by individuals following a data breach.

Entities, in assessing the data breach, should clearly establish what information was involved in the data breach, including whether the breach involved 'sensitive information'[29] (such as information about an individual's health), government related identifiers (such as a Medicare number or driver licence number), or financial information.

Steps recommended to individuals in response to the eligible data breach

The statement must include recommendations individuals should take in response to the data breach, to mitigate the serious harm or likelihood of serious harm from the data breach.

The nature of recommendations will depend on the entity's functions and activities, the circumstances of the eligible data breach, and the kind or kinds of information that were involved. Recommendations should include practical steps that are easy for the individuals to action.

For example, to help reduce the risk of identity theft or fraud, recommendations in response to a data breach that involved individuals' Medicare numbers might include steps an individual can take to request a new Medicare card. Or in the case of a data breach that involved credit card information, putting individuals at risk of identity theft, recommendations might include that an individual contact their financial institution to change their credit card number, and also contact a credit reporting body to establish a ban period on their credit report.

Where the entity does not have the requisite knowledge or capacity to provide advice to affected individuals, they should seek specialist advice or assistance in preparing this section. In limited circumstances, after seeking advice, the entity may use this section to advise individuals that no steps are required.

[29] See s 6(1) of the Privacy Act for categories of personal information that are covered by the definition of 'sensitive information'.

Additional information to provide

Other entities involved in the data breach

If more than one entity holds personal information that was compromised in an eligible data breach, only one entity needs to prepare a statement and notify individuals about the data breach (s 26WM, and see *Data breaches involving more than one entity).* This may occur when an entity outsources the handling of personal information, is involved in a joint venture, or where it has a shared services arrangement with another entity.

When a data breach affects more than one entity, the entity that prepares the statement may include the identity and contact details of the other entities involved (s 26WK(4)). Whether an entity includes the identity and contact details of other involved entities in its statement will depend on the circumstances of the eligible data breach, and the relationship between the entities and the individuals involved. The Privacy Act does not require this information to be included on the statement, and it is open to entities to assess whether it is useful to provide this information to individuals.

The OAIC recognises that in some instances the identity and contact details of a third party may not be relevant to an individual whose personal information is involved in an eligible data breach, for example, where the individual does not have a relationship with the other entity. In these circumstances, rather than include the identity and contact details of the third party or parties, the entity that prepares the statement may wish to describe the nature of the relationship with the third party in its description of the data breach.

When to provide a copy of the statement to the Commissioner

Entities must prepare and give a copy of the statement to the Commissioner as soon as practicable after becoming aware of the eligible data breach (s 26WK(2)).

What is a 'practicable' timeframe will vary depending on the entity's circumstances, and may include considerations of the time, effort, or cost required to prepare the statement. The OAIC expects that once an entity becomes aware of an eligible data breach, it will provide a statement to the Commissioner promptly, unless there are circumstances that reasonably hinder the entity's ability to do so.

It may be appropriate in some circumstances for an entity to advise individuals about the contents of the statement before or at the same time that it gives the statement to the Commissioner, rather than waiting.

While a statement provided to the Commissioner and individuals must include certain information outlined above (s 26WK(3)), where additional relevant information becomes available after submitting this statement, the entity may provide this to the OAIC. The OAIC will include instructions about how to provide any supplementary information upon receipt of the statement.

How to provide the statement to the Commissioner

The OAIC has an online form for entities to lodge all eligible date breach statements under section 26WK of the Privacy Act.

If you are unable to use the online form, please contact the OAIC enquiries line to make alternative arrangements.

Australian Information Commissioner's role in the NDB scheme

Key points

The Commissioner has a number of roles under the NDB scheme in the Privacy Act. These include:

- receiving notifications of eligible data breaches
- encouraging compliance with the scheme, including by handling complaints, conducting investigations, and taking other regulatory action in response to instances of non-compliance
- offering advice and guidance to regulated entities, and providing information to the community about the operation of the scheme.

This document summarises how the Commissioner anticipates exercising these functions. For more information about the Commissioner's regulatory powers and how those powers are exercised, see the OAIC's *Privacy regulation action policy*[30] and the *Guide to privacy regulatory action*.[31]

Notifications of data breaches to the Commissioner

How to notify the Commissioner

Once an entity has reasonable grounds to believe there has been an eligible data breach and it is not exempted from notifying, it is required to provide notification to individuals at risk of serious harm and the Commissioner. When notifying the Commissioner, the entity must provide a notification statement that contains the following information (s 26WK(3)):

1. The identity and contact details of the notifying entity.
2. A description of the data breach.
3. The kind or kinds of information concerned.
4. Recommendations to individuals about the steps that they should take to minimise the impact of the breach.

An online form is available on the OAIC website to help entities lodge notification statements and provide additional supporting information (see *What to include in an eligible data breach statement*).

Providing voluntary information

Although not required by the Privacy Act, entities may provide additional supporting information to the Commissioner to explain the circumstances of the data breach and the entity's response in further detail. For example, entities may choose to provide the Commissioner with technical

---

[30] The *Privacy regulatory action policy* explains the OAIC's approach to using its privacy regulatory powers and communicating information publicly. Available online at www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/.

[31] The *Guide to privacy regulatory action* sets out a detailed explanation of particular privacy regulatory powers, looking at the legislative framework and purpose of the power, and the procedural steps the OAIC will take in the exercise of the regulatory power. Available online at www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/.

information, which may not be appropriate to include in the statement to individuals. This information will assist the Commissioner to decide whether to make further inquiries or to take any other action. It may also be used by the Commissioner when preparing statistical reports about notifications received.

When a data breach affects more than one entity, the entity that prepares the statement may also choose to include the identity and contact details of the other entities involved (s 26WK(4)). The Privacy Act does not require this information to be included on the statement, and it is open to entities to assess whether it is useful to provide this information in the statement.

Confidentiality of information provided in notifications

If an entity elects to provide additional supporting information to the Commissioner, it may request that the Commissioner hold that information in confidence. The Commissioner will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose such information after consulting with the notifying entity, and with the entity's agreement or where required by law.

If the Commissioner receives a freedom of information (FOI) request for a notification statement or additional supporting information, the Commissioner will consult with the entity that made the notification before responding. As a matter of course, the Commissioner will offer to transfer any FOI requests relating to agencies to the agencies in question.

The Commissioner's response to notifications

The Commissioner will acknowledge receipt of all data breach notifications.

The Commissioner may also make inquiries or offer advice and guidance in response to notifications. In deciding whether to make inquiries or offer advice and guidance in response to a notification, the Commissioner may consider the type and sensitivity of the personal information, the numbers of individuals potentially at risk of serious harm, and the extent to which the notification statement and any additional supporting information provided demonstrate that:

- the data breach has been contained or is in the process of being contained where feasible
- the notifying entity has taken, or is taking, reasonable steps to mitigate the impact of the breach on the individuals at risk of serious harm
- the entity has taken, or is taking, reasonable steps to minimise the likelihood of a similar breach occurring again.

The Commissioner may also decide to take regulatory action on the Commissioner's own initiative in response to a notification, or a series of notifications. In deciding whether to take regulatory action, the Commissioner will have regard to the OAIC's Privacy regulatory action policy and Guide to privacy regulatory action.

However, generally the Commissioner's priority when responding to notifications is to provide guidance to the entity and to assist individuals at risk of serious harm.

The Commissioner's enforcement of the NDB scheme

The Commissioner has a number of enforcement powers to ensure that entities meet their obligations under the scheme. A failure by an entity to meet any of the following requirements of the scheme is an interference with the privacy of an individual (s 13(4A)):

- Conduct a reasonable and expeditious assessment of a suspected eligible data breach (s 26WH(2)), taking all reasonable steps to ensure that this assessment is completed within 30 days of becoming aware (s 26WH(2)(b)).
- Prepare a statement about the data breach, and give a copy to the Commissioner, as soon as practicable (s 26WK(2)).
- Notify the contents of the statement to individuals at risk of serious harm (or, in certain circumstances, publish the statement) as soon as practicable (s 26WL(3)).
- Comply with a direction from the Commissioner to prepare a statement and notify as soon as practicable (s 26WR(10)).

The enforcement powers available to the Commissioner in response to an interference with privacy, which range from less serious to more serious regulatory action, include powers to:

- accept an enforceable undertaking (s 33E) and bring proceedings to enforce an enforceable undertaking (s 33F)
- make a determination (s 52) and bring proceedings to enforce a determination (ss 55A and 62)
- seek an injunction to prevent ongoing activity or a recurrence (s 98)
- apply to court for a civil penalty order for a breach of a civil penalty provision (s 80W), which includes a serious or repeated interference with privacy (s 13G). [32]

The Commissioner is also required, in most circumstances, to investigate a complaint made by an individual about an interference with the individual's privacy (s 36), which would include a failure to notify an individual at risk of serious harm of an eligible data breach where required to do so.

In deciding when to exercise enforcement powers in relation to a contravention of the NDB scheme, the Commissioner will have regard to the OAIC's Privacy Regulatory Action Policy and the circumstances outlined in Chapter 9: Data breach incidents of the OAIC's Guide to privacy regulatory action.

The preferred approach of the Commissioner is to work with entities to encourage and facilitate compliance with an entity's obligations under the Privacy Act before taking enforcement action.

The Commissioner acknowledges that it will take time for all regulated entities to become familiar with the requirements of the NDB scheme. During the first 12 months of the scheme's operation, the Commissioner's primary focus will be on working with entities to ensure that they understand the new requirements and are working in good faith to implement them.

[32] For more information about civil penalty provisions in the Privacy Act, see *Guide to privacy regulatory action,* Chapter 6: Civil Penalties – serious or repeated interference with privacy and other penalty provisions.

The Commissioner's other powers and functions under the scheme

Direction to notify (s 26WR)

The Commissioner can direct an entity to notify individuals at risk of serious harm, as well as the Commissioner, about an eligible data breach in certain circumstances.

Before directing an entity to notify, the Commissioner will usually ask the entity to agree to notify. This might happen if a data breach comes to the attention of the Commissioner but has not come to the attention of the relevant entity, or if the Commissioner does not agree with the entity's initial view about whether a data breach triggers an obligation to notify.

If the Commissioner and the entity cannot agree about whether notification should occur, the Commissioner will give the entity an opportunity to make a formal submission about why notification is not required, or if notification is required, on what terms. The Commissioner will consider the submission and any other relevant information before deciding whether to direct the entity to notify under s 26WR.

Declaration that notification need not be made, or that notification be delayed (s 26WQ)

The Commissioner may declare that notification of a particular data breach is not required (s 26WQ(1)(c)). The Commissioner may also modify the period in which notification needs to occur (s 26WQ(1)(d)).

The Commissioner cannot make a declaration under s 26WQ unless satisfied that it is reasonable in the circumstances to do so, having regard to the public interest, any relevant advice received from an enforcement body or the Australian Signals Directorate, and any other relevant matter. While the Commissioner is empowered to make a declaration if it is 'reasonable in the circumstances to do so', the Commissioner still has discretion about whether to make a declaration, and on what terms.

In deciding whether to make a declaration, and on what terms, the Commissioner will have regard to the objects of the Privacy Act (s 2A) and other relevant matters. The Commissioner will consider whether the risks associated with notifying a particular data breach outweigh the benefits of notification to individuals at risk of serious harm.

Given the clear objective of the scheme to promote notification of eligible data breaches to affected individuals, and the inclusion of exceptions in the scheme that remove the need to notify in a wide range of circumstances, the Commissioner expects that declarations under s 26WQ will be limited to exceptional cases.

An entity applying for a declaration will be expected to make a well-reasoned and convincing case detailing how the data breach is an eligible data breach, why any relevant exceptions do not apply, and why notification should not occur or should be delayed. The entity should provide detailed evidence or information in support of its application.

Advice, guidance, and community information

The Commissioner provides general information to the community about the Privacy Act, including the NDB scheme, via the OAIC's website or its public enquiries service.

The Commissioner has developed this guide and other resources, which are available on the OAIC's website, to help entities comply with the scheme.

However, the Commissioner will not be able to provide detailed advice about the application of the scheme to specific data breaches. Entities should seek their own legal and technical advice.

Part of the Commissioner's role in the NDB scheme is to promote transparency in the way that entities handle personal information. To this end, the Commissioner will regularly publish de-identified statistical information about data breaches notified under the scheme.

Part 5: Other sources of information

This guide has focussed on how to manage data breaches affecting personal information for entities with obligations under the Privacy Act.

Entities may need to consider whether the circumstances of a data breach triggers other requirements, or if the type of information that they hold warrants specific actions to prepare for and manage a data breach. For instance, it may be appropriate to seek advice from the Australian Taxation Office for a data breach that involves tax file numbers; or to seek guidance from the Australian Digital Health Agency if a data breach involves information stored in the My Health Record system.

Entities may also be required to notify other regulators about certain matters under industry-specific regulation; or to notify professional associations about matters related to a data breach. Contractual arrangements may also create obligations to do certain things to prepare for a data breach, and to share certain information in the event of a data breach.

Relevant sources of advice in the event of a data breach (in addition to the Commissioner) may include:

- federal or State or Territory police or law enforcement bodies
- the affected entity's financial services provider
- Australian Securities & Investments Commission (ASIC)
- Australian Prudential Regulation Authority (APRA)
- Australian Taxation Office (ATO)
- Australian Cyber Security Centre (ACSC)[33]
- CERT Australia
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Digital Health Agency (ADHA)[34]
- Department of Health[35]
- State or Territory Privacy and Information Commissioners[36]
- IDcare, or other organisations that support individuals affected by data breaches
- professional associations and professional regulatory bodies
- third parties under an agreement or contract, for example contracted service providers or insurance providers.

---

[33] Further information about cyber security incidents that should be reported is available at www.asd.gov.au/infosec/reportincident.htm.

[34] For data breaches involving the My Health Record system.

[35] For data breaches involving the National Cancer Screening Register.

[36] For more information about state and territory jurisdictions see www.oaic.gov.au/privacy-law/other-privacy-jurisdictions.

Other OAIC resources

- *Guide to securing personal information*
- Chapter 9: Data breach incidents in the *Guide to privacy regulatory action*
- Chapter 1 and Chapter 11 of the *APP guidelines*
- Consumer resources: *What to do after a data breach* and *Receiving data breach notifications*
- *Guide to mandatory data breach notification in the My Health Record system*

Cyber security resources

Technical standards and guidance that may assist entities to prepare for and respond to a data breach include the following:

- CERT Australia, Australia's national computer emergency response team - CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.
- International standards published by the International Organization for Standardization (ISO) and Australian standards published by Standards Australia (see also the 'Standards' section in Part D of this guide), including the AS/NZS ISO/IEC 27000 series of information security management standards
- National Institute of Standards and Technology (USA), provides detailed frameworks based on ISO standards (https://www.nist.gov/topics/cybersecurity)
- *Control Objectives for Information and Related Technology* (COBIT) — COBIT 5 is the latest edition of Information Systems Audit and Control Association's (ISACA) international framework for information technology (IT) management and IT governance.
- The *National eHealth Security and Access Framework* (NESAF) is a comprehensive suite of documents regarding health security for the health industry and specific Australian health organisations. The NESAF aims to assist health organisations in meeting their security obligations.

The following resources are particularly relevant to Australian Government agencies but are also useful for other organisations and government agencies:

- *Australian Government Protective Security Policy Framework* (PSPF), aims to enhance Australia's information security culture and provide a common approach to the implementation of protective security by Australian Government agencies. The PSPF may also be used by other government agencies (including State and Territory agencies), as well as the private sector as a model for better security practice
- Australian Signals Directorate (ASD), publishes a range of ICT security publications including the *Australian Government Information Security Manual*, *Preparing for and Responding to Cyber Security Incidents*, *Cyber Security Incidents – Are you Ready?*, and *Strategies to Mitigate Cyber Security Incidents*
- Australian Cyber Security Centre provides a range of resources on cyber security for businesses, individuals and government.

Appendix A: Key terms

Agency is defined in s 6(1) of the Privacy Act and includes most Australian Government agencies, agencies and Ministers.

APPs are the Australian Privacy Principles set out Schedule 1 to the Privacy Act, which apply to APP entities.

APP entity is defined in s 6(1) of the Privacy Act to mean an agency or organisation.

Assessment is a key step in responding to a data breach, which should enable entities to make an evidence-based decision about whether serious harm is likely. Entities that are subject to the NDB scheme are required to conduct assessments of suspected eligible data breaches under s 26WH of the Privacy Act.

Australian Information Commissioner, administers the Privacy Act, and is appointed under s 14 of the *Australian Information Commissioner Act 2010* (Cth).

Credit provider is defined in s 6(1) of the Privacy Act

Credit reporting body is defined in s 6(1) of the Privacy Act and generally applies to a business or undertaking that involves collecting, holding, using, or disclosing personal information about individuals for the purpose of providing an entity with information about the credit worthiness of an individual (s 6P of the Privacy Act).

Data breach is the unauthorised access or disclosure of personal information, or loss of personal information.

Eligible data breach is the unauthorised access or disclosure of personal information, or loss of personal information in circumstances where this is likely to occur, that is likely to result in serious harm to any of the individuals to whom the information relates (see s 26WE(2) of the Privacy Act).

Enforcement body is a body listed in s 6(1) of the Privacy Act.

Enforcement related activities are functions listed in s 6(1) of the Privacy Act.

Entity is an agency, organisation, credit reporting body, credit provider, or file number recipient that has obligations under s 26WE(1) of the Privacy Act.

File number recipient is defined in s 11 of the Privacy Act as a person in possession or control of a record that contains a tax file number.

Health service is defined in s 6FB of the Privacy Act, and includes general activities to assess, maintain or improve an individual's health.

My Health Records Act is the *My Health Records Act 2012* (Cth).

NDB scheme is the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

Notifiable data breach is the same as eligible data breach.

Notification statement is a statement about an eligible data breach, prepared by an entity under s 26WK.

OAIC is the Office of the Australian Information Commissioner.

Organisation is defined in s 6C of the Privacy Act, and includes all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers and some small businesses (see s 6D and 6E of the Privacy Act).

Privacy Act is the *Privacy Act 1988* (Cth).

Personal information is defined in s 6(1) of the Privacy Act, as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Remedial action is the steps that an entity may take to prevent the likelihood of serious harm occurring for any individuals whose personal information is involved in an eligible data breach.

Sensitive information is defined in s 6(1) of the Privacy Act to include personal information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. Sensitive information also includes all health information, genetic information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.

Small business operator is defined in s 6D of the Privacy Act.

State or Territory authority is defined in s 6C(3) of the Privacy Act.

TFN means Tax File Number, as defined in s 6(1) of the Privacy Act.