Australian Government
Office of the Australian Information Commissioner

May 2017

# Identifying eligible data breaches

The Office of the Australian Information Commissioner (OAIC) published this resource as an exposure draft on 2 June 2017. The OAIC would welcome comments from any interested parties about this resource before it is finalised. If you would like to provide comment on this resource, please email **consultation@oaic.gov.au** by 14 July 2017.

» Further information on providing comment

## Key points

- The notifiable data breaches (NDB) scheme requires regulated entities (entities) to notify particular individuals and the OAIC 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 OAIC. 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. The OAIC will develop a separate resource, *Assessing a suspected data breach*, to provide 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 1988* (Cth) (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).

  For example, an employee browses sensitive customer records without any legitimate purpose, or a computer network is compromised by an external attacker resulting in personal information being accessed without authority.

- ***Unauthorised disclosure*** occurs when an entity 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 publishes a confidential data file containing the personal information of one or more individuals on the internet.

- ***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 a notifiable 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. What is reasonable can be influenced by relevant standards and practices. 'Reasonable

person' is also discussed in general terms in Chapter B of the OAIC's *Australian Privacy Principle Guidelines*.[1]

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

The chance that an individual will experience serious harm increases as the number of people whose personal information was part of the data breach increases. It may therefore be prudent for an entity to assume that a data breach that involves the loss of personal information of a very large number of individuals is likely to result in serious harm to at least one of those individuals unless the context or circumstances would support this not being the case.

'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' 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

[1] Available at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts.

- 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 are 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',[2] such as information about an individual's health
- documents commonly used for identity fraud (including Medicare card, driver licence, and passport details)
- financial information
- a combination of personal information (rather than a single piece of personal information).

## 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 (such as young persons and vulnerable individuals) 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 a vulnerable segment of the community, 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 may 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 enough people's personal information is involved in the breach, it may become likely that some of the individuals will experience serious harm. From a risk perspective, it may be prudent, depending on the particular circumstances, to treat a breach involving the personal information of a very large number of people as likely to result in serious harm to at least one of those individuals.
- **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

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

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 physical or mental health service.[3]

- **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 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 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 that prevents the likelihood of serious

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

harm occurring for any individuals whose personal information is involved in the data breach, 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 the unauthorised access 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 sender then confirms that the recipient has not copied, and has permanently deleted the data file.

**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.[4] However, whether any data breach is notifiable depends on the particular circumstances of the breach.

**Example 1 — strong encryption making notification unnecessary**

WeCare, 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

[4] The acts and practices described in these examples may raise other compliance issues under the Privacy Act, such as whether an APP entity has complied with relevant Australian Privacy Principles.

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.

WeCare 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. WeCare implemented the recommendations of the IT security consultant, including new IT security protocols and intrusion detection software.

WeCare 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, WeCare decides it is not an eligible data breach, and does not notify the OAIC or the affected individuals.

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.

**Example 2 — notification following unintentional publication of sensitive data**

PharmaChoice, 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. PharmaChoice's security consultants identify that the database was publicly available for a limited time and that it was only accessed a few times.

However, PharmaChoice 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, PharmaChoice's risk assessment concludes that the data breach would be likely to result in serious harm to some of its customers.

PharmaChoice decides to notify all customers whose personal information is involved in the data breach. 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**

Shop4You 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 Shop4You have been downloaded by an external IP address. The bulk mailing distributions lists include the name, email address, gender, and suburb of Shop4You's customers. The service provider notifies Shop4You, who conducts an immediate investigation into how the mailing lists were accessed and downloaded.

An IT Security sweep detects malware on an employee's computer, and the investigation concludes that their login credentials were obtained after the employee unintentionally opened an email attachment from a malicious third party attacker. As Shop4You also held the personal information, assuming that the service provider was not an APP entity, Shop4You undertook an assessment of whether it was required to notify individuals and the OAIC.

As part of its assessment, Shop4You identified that some of the individuals whose personal information was involved in the data breach received emails that fraudulently claimed to be sent from Shop4You, and which sought to obtain the individual's credit card details. As a result, Shop4You concludes that it is more probable than not that the attacker will use the information in the mailing lists for the purposes of 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, Shop4You notifies the OAIC and sends an email with the relevant information required by the NDB scheme to those individuals whose personal information is involved in the data breach. Shop4You's 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 memory stick containing the employee records of 200 employees of an Australian Government Department (the Department) goes missing while the employee who holds the memory stick is travelling from one work site to another. Once the Department becomes aware that the memory stick is lost, it conducts an extensive search but fails to locate it. The information contained in the employee records 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, and there is a chance that the memory stick was lost outside of the Department's premises, the Department concludes that unauthorised disclosure 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 OAIC.

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 OAIC. 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**

Jupiter 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, Jupiter 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 Jupiter 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, Jupiter Bank does not notify the OAIC.

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

Care Services, 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 Care Services 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.

The Care Services employee realises the error, and contacts Business B to delete the email with the attachment. Business B confirms it has not accessed the file, and that it has deleted the email. Care Services' assessment of the remedial action taken concludes that, while the file included sensitive information about the individuals' health, the assurance that Business B deleted the file has prevented the likely risk of serious harm to any individuals. As a consequence, Care Services determines that it is not an eligible data breach that needs to be notified.



## For further information

GPO Box 5218 Sydney NSW 2001 | **P** 1300 363 992 | **E** enquiries@oaic.gov.au

**Or visit our website www.oaic.gov.au**

*The information provided in this resource is of a general nature. It is not a substitute for legal advice.*