national museum australia

Data breach response procedures

PRO-030

Version no.1.0 27 February 2018

Contents

1. Title 3
2. Scope 3
2.1 Purpose 3
2.2 Background 3
3. Procedures 3
3.1 What is a data breach? 3
3.2 Which data breaches must be notified? 4
3.3 What does 'likely to result in serious harm' mean? 4
3.4 Who decides if a data breach is likely to result in serious harm? 4
3.5 What to do if a data breach is suspected but not confirmed 5
3.6 Who should the data breach be reported to? 5
3.7 Remedial action 6
3.8 Establishing a data breach response team 6
3.9 Record keeping 7
3.10 How should notification occur? 7
3.11 Review and follow up 8
4. Definition of terms 8
5. Definition of responsibilities 8
6. Relevant policies 8
7. Implementation 9
7.1 Coverage 9
7.2 Other related procedures 9
7.3 Exclusions 9
7.4 Monitoring 9
8. Attachments 9

ID	PRO-030
Version	1.0
Version date	27 February 2018
Approved by	Executive Management Group
Approval date	27 February 2018
File	18/63
Availability	Public and all museum staff, contractors and volunteers
Keywords	Privacy – personal information – notifiable data breaches scheme
Responsible officer	Privacy Contact Officer
History	
Key changes	
Review date	February 2020
Related documents	Privacy Policy Information Security Policy *Privacy Act 1988* (Cth)
Contact	National Museum of Australia GPO Box 1901 CANBERRA ACT 2601 p: (02) 6208 5000 e: information@nma.gov.au web: www.nma.gov.au

1. Title

Data breach response procedures

2. Scope

2.1 Purpose

This data breach response procedure sets out the procedures that National Museum of Australia staff must follow if the Museum experiences an actual or suspected data breach. It explains key responsibilities and actions to be taken.

These procedures will help staff contain, assess and respond to data breaches quickly and in a way that mitigates harm to affected individuals. It will also help the Museum to meets its obligations under the Notifiable Data Breaches (NDB) scheme and give confidence to employees and customers that the Museum treats their personal information seriously, and will respond promptly and quickly to protect it.

2.2 Background

The NDB scheme came into effect on 22 February 2018. It applies to all agencies and organisations covered by the *Privacy Act 1988*, which includes the Museum. Under the scheme, the Museum must notify individuals whose personal information is involved in certain data breaches, and the Australian Information Commissioner, about the breach.

3. Procedures

3.1 What is a data breach?

A data breach occurs when there has been unauthorised access to, or unauthorised disclosure of, personal information or a loss of personal information.

Unauthorised access occurs when personal information is accessed by someone who is not permitted to do so. This includes access by an employee, independent contractor, or an external third party such as a hacker.

- Examples: An employee browses sensitive customer records without legitimate reason. Personal information is accessed in an external IT attack.

Unauthorised disclosure involves personal information being made available (intentionally or unintentionally) to others outside the Museum.

- Example: A person accidentally emails a spreadsheet containing credit card details to the wrong recipient in another organisation.

Loss of personal information is the loss of personal information, where that information can be accessed or disclosed.

- Examples: An unencrypted USB stick containing a spreadsheet of personal information is left on public transport. Hard copy employee records are found in an unsecured bin at a public waste facility.

3.2 Which data breaches must be notified?

The NDB scheme establishes a notification scheme for data breaches that are likely to result in serious harm. Under the scheme, individuals whose personal information is involved in such data breaches must be notified of the breach and the steps taken in response to the breach. The Australian Information Commissioner must also be notified of the data breach.

If the Museum has responded quickly to the breach, and as a result of this action the data breach is not likely to result in serious harm, there is no need to notify individuals or the Australian Information Commissioner. However, the Museum may decide to tell individuals about the incident if it is considered appropriate.

3.3 What does 'likely to result in serious harm' mean?

An assessment must be made of whether a data breach is *likely to result in serious harm* to any of the individuals to whom the information relates. Although 'serious harm' is not defined in the Privacy Act, it would encompass serious physical, psychological, emotional, financial or reputational harm. The risk of serious harm should be assessed by considering both the *likelihood* of the harm occurring and the *consequences* of the harm. Some of the factors that should be considered are:

(i) The type of personal information involved in the data breach

Some personal information is more sensitive than other information and could lead to serious ramifications for individuals if accessed. Information about a person's health, documents commonly used for identity fraud (for example Medicare card, driver's licence) or financial information are examples of information that could be misused if the information falls into the wrong hands.

(ii) Circumstances of the data breach

The scale and size of the breach may be relevant in determining the likelihood of serious harm. The disclosure of information relating to a large number of individuals would normally lead to a higher risk of at least some of those people experiencing harm. The length of time that the information has been accessible is also relevant.

Think about who may have gained unauthorised access to information, and what their intention was (if any) in obtaining such access. It may be that there was a specific intention to use the information in a negative or malicious way.

(iii) Nature of possible harm

Consider the broad range of potential harm that could follow from a data breach including:

- identity theft
- financial loss
- threat to a person's safety
- loss of business or employment opportunities
- damage to reputation (personal and professional).

3.4 Who decides if a data breach is likely to result in serious harm?

Only one of the following Museum representatives should make an assessment of whether there is a likelihood of serious harm in relation to a particular data breach:

- Privacy Contact Officer
- Information Security Advisor

- Agency Security Advisor
- Chief Information Officer
- HR Manager
- People Strategy Manager
- Deputy Director
- Associate Director
- Chief Operating Officer
- Director.

The Australian Information Commissioner has enforcement powers under Privacy Act including receiving complaints from individuals, conducting investigations and issuing directions to an agency. Given these consequences of non-compliance with the NDB scheme, only the Museum staff listed above are responsible for determining whether a data breach is likely to result in serious harm and should be notified under the scheme.

3.5 What to do if a data breach is suspected but not confirmed

The notification requirements apply where there are reasonable grounds for believing that a data breach has occurred.

If it is unclear whether a data breach has occurred, but there is a suspicion that there may have been a breach, staff need to act quickly. Once it is suspected that there may have been a breach, the Privacy Act requires that an assessment of the situation be made as soon as practicable (within 30 days) to determine if there has been a data breach requiring notification.

The assessment process should involve:

- deciding whether an assessment is necessary and who should carry it out
- quickly gathering relevant information about the suspected breach
- deciding whether an eligible data breach has occurred and if so, following these procedures.

Remember that steps can be taken to mitigate potential harm at any time. If remedial action is successful in preventing serious harm, notification is not required.

3.6 Who should the data breach be reported to?

Staff who initially become aware that a data breach has occurred, or suspect that one has occurred, must immediately inform their business unit manager. They should make a record of:

- the time and date the breach was discovered or suspected
- the type of personal information involved
- the cause and extent of the breach
- any other relevant information.

If a data breach is suspected the business unit manager (or nominee) should conduct an assessment as referred to in paragraph 3.5.

If a data breach is known to have happened, the staff member and/or their business unite manager must advise the Privacy Contact Officer and relevant Deputy Director, Chief Operating Officer or Associate Director as soon as practicable.

3.7 Remedial action

Action should be taken as soon as possible to contain a suspected or known breach. This involves taking immediate steps to limit any further access to or distribution of the information. Such action might involve recovering or locating lost information before it is accessed or changing controls on IT accounts.

There is no need to notify individuals or the Australian Information Commissioner of data breaches if the Museum has taken remedial action, and as a result the data breach would not be likely to result in serious harm. Whether the remedial action is sufficient should be considered in the earliest stages of the data breach by the Museum representative listed in paragraph 3.4, in consultation with the Privacy Contact Officer.

3.8 Establishing a data breach response team

A data breach response team should be established as soon as possible once it is determined that a data breach is likely to require notification of affected individuals.

The role of the response team is to:

- take action to contain the breach
- ensure evidence/information is collected and preserved
- conduct an investigation to determine when and how the breach occurred, the type of information involved, the cause and extent of the breach, the individuals affected and the risk of serious harm
- decide who needs to be made aware of the breach
- decide whether to notify affected individuals, how the notification should occur and the contents of the notification and
- report to the Executive on the outcome of the investigation and any recommendations.

The Privacy Contact Officer will coordinate the team's response and advise the Executive as required. If the Privacy Contact Officer is unavailable the Chief Information Officer or nominee will take on this role.

The composition of the response team will depend on the size, nature and complexity of the breach. Representatives of the business unit responsible for the personal information involved in the data breach would usually be a part of the response team. For example a data breach relating to the Friends membership program would mean that the business unit administering the Friends program would be represented on the response team. In addition, the following staff members or their nominees would play a role if the data breach related to the matters outlined in the table below:

Position	Subject matter of data breach
Chief Information Officer or IT Security Advisor	Breach relates to the Museum's IT system or telecommunications network
HR Manager or People Strategy Manager	Breach relates to HR functions or large-scale disclosure of employee information
Agency Security Advisor	Breach relates to the Museum's security system or otherwise raises security issues

Chief Operating Officer	Breach involves several corporate business units, raises systemic IT or security issues, or relates to the Corporate and Cultural Shared Services Centre (CCSSC)
Public Affairs Manager	If there is likely to be media or stakeholder attention as a result of the breach

If the data breach involves personal information relating to customers or employees of an agency receiving services from the CCSSC, a representative of that agency should be involved. Where required, expert external advice (for example specialised IT security services) may also be sought if not available within the Museum.

3.9 Record keeping

Records of the data breach and the response team's actions should be kept in a CM9 file. The CM9 file should have security controls applied so that access to any documents containing personal information (including material detailing the subject matter of the breach) is restricted to those staff members who need to have access to the information.

3.10 How should notification occur?

Where serious harm is likely, the Privacy Contact Officer will advise the Australian Information Commissioner of the type of breach, the information it relates to and recommended steps for individuals to minimise the risk of serious harm.

A similar notification must be provided to the affected individuals. There are three options for notifying individuals:

1. Notify all individuals whose personal information is affected
2. Notify only those individuals at risk of serious harm
3. If neither of the above are practicable, publish a statement on the Museum's website and further publicise it via other means, for example social media or media release.

Deciding which option to use to notify individuals will depend on the time, effort and cost involved. If it is not possible to assess which particular individuals are at risk of serious harm, all individuals who are impacted by the breach should be notified. Where the response team determines that only a subset of people are at risk of harm, it may be better to notify only those individuals to avoid causing unnecessary distress to individuals who are not at risk.

Individuals should be contacted using the method of communication normally used by the Museum to communicate with them. Individuals can be notified by email, SMS, telephone call or letter. If contact details for the person are available, direct communication is appropriate. If contact details are not available then a message on the Museum's website or via social medial channels may be the best way of notifying affected individuals.

The notification must include as a minimum the following:

- the name and contact details of the Museum
- a description of the data breach including when it occurred, the circumstances of the breach, who may have accessed the information and the steps taken to contain the breach
- the kinds of information concerned

- recommendations about the practical steps (if any) that affected people should take in response to the breach.

3.11 Review and follow up

The response team should review the incident and make recommendations about how to prevent future breaches. This may include updating policies or procedures, revising or conducting additional staff training or changing IT access controls. Where additional risks are discovered through a data breach, relevant policies or procedures (such as security risk management plans or threat risk assessments) should be updated to reflect the new risk or threat and potential mitigations.

4. Definition of terms

Data breach means unauthorised access to, or unauthorised disclosure of, personal information or a loss of personal information.

Notifiable data breach means a data breach that is likely to result in serious harm, which must be notified to affected individuals and the Australian Information Commissioner.

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not and
(b) whether the information or opinion is recorded in a material form or not.

5. Definition of responsibilities

Australian Information Commissioner is responsible for receiving notifications of eligible data breaches, encouraging compliance with the NDB scheme, handling complaints, conducting investigations, and taking action in response to non-compliance.

Privacy Contact Officer is responsible for maintaining these procedures. The Privacy Contact Officer is also responsible for providing advice on privacy issues, acting as the point of contact for the Australian Information Commissioner and investigating privacy complaints.

6. Relevant policies

This procedure supports the following policies:

- Privacy Policy
- IT Security Policy
- Telecommunications policy
- Mail handling policy
- IT Acceptable Use Conditions.

7. Implementation

7.1 Coverage
Whole of Museum

7.2 Other related procedures
Not applicable

7.3 Exclusions
Not applicable

7.4 Monitoring
These procedures will be reviewed in 2020, or earlier if the need arises.

8. Attachments

Not applicable