Australian Government
Attorney-General's Department

AGD Data Breach Response Plan

November | 2018

ISBN: 978-1-920838-67-6 (Online)

Contents

Introduction

This data breach response plan (response plan) sets out procedures and clear lines of authority for Attorney General's Department (AGD) staff in the event of a data breach or suspected data breach.

Consistent with good privacy practice, this response plan also covers unauthorised use, modification or interference with personal information held by AGD. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals and entities.

What is a Data Breach?

A data breach occurs when personal information is lost or subjected to unauthorised access or disclosure. Information that is not, on the face of it, about an individual can be personal information if, when combined with other information, an individual is 'reasonably identifiable'.

A data breach may be malicious, or the result of human error or a failure in information handling or security systems, and could include:

- theft of a document containing personal information
- sending an email containing personal information to the wrong person
- inadequate identity verification procedures resulting in the disclosure of personal information to a scammer.

What is a Notifiable Data Breach?

Part IIIC of the *Privacy Act 1988* establishes the Notifiable Data Breach (NDB) scheme. The NDB scheme is designed to enhance accountability for privacy protection and ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm.

Under the NDB scheme, an 'eligible data breach' occurs where:

- personal information is lost (in circumstances where unauthorised access or disclosure is likely to result) or is subjected to unauthorised access or disclosure, and
- the loss, access or disclosure is likely to result in serious harm to one or more individuals to whom the information relates, and
- the entity has been unable to prevent the likely risk of serious harm with remedial action.

Where an eligible data breach occurs or is suspected, AGD is required to notify both affected individuals and the Office of the Australian Information Commissioner (OAIC).

Purpose of this Plan

This response plan is intended to enable AGD to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the NDB scheme that commenced on 22 February 2018. Actions taken in the first 24 hours after discovering a data breach or suspected data breach are crucial to the success of our response.

The plan sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist AGD to respond to a data breach.

Process Flow Chart

AGD, AGD Contractor or third party who collects personal information on behalf of the department experiences data breach/data breach suspected

Discovered by AGD staff member, contractor or AGD staff member, or otherwise alerted by a third party who collects personal information on behalf of the department.

What should the AGD staff member do?

- Immediately notify your supervisor of the suspected data breach. AGD contractors and third parties are to notify their respective contact area within the department or the AGD Privacy Unit.
- Record and advise your supervisor (or if a contractor or third party notify the AGD Privacy Unit) of the time and date the suspected breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.

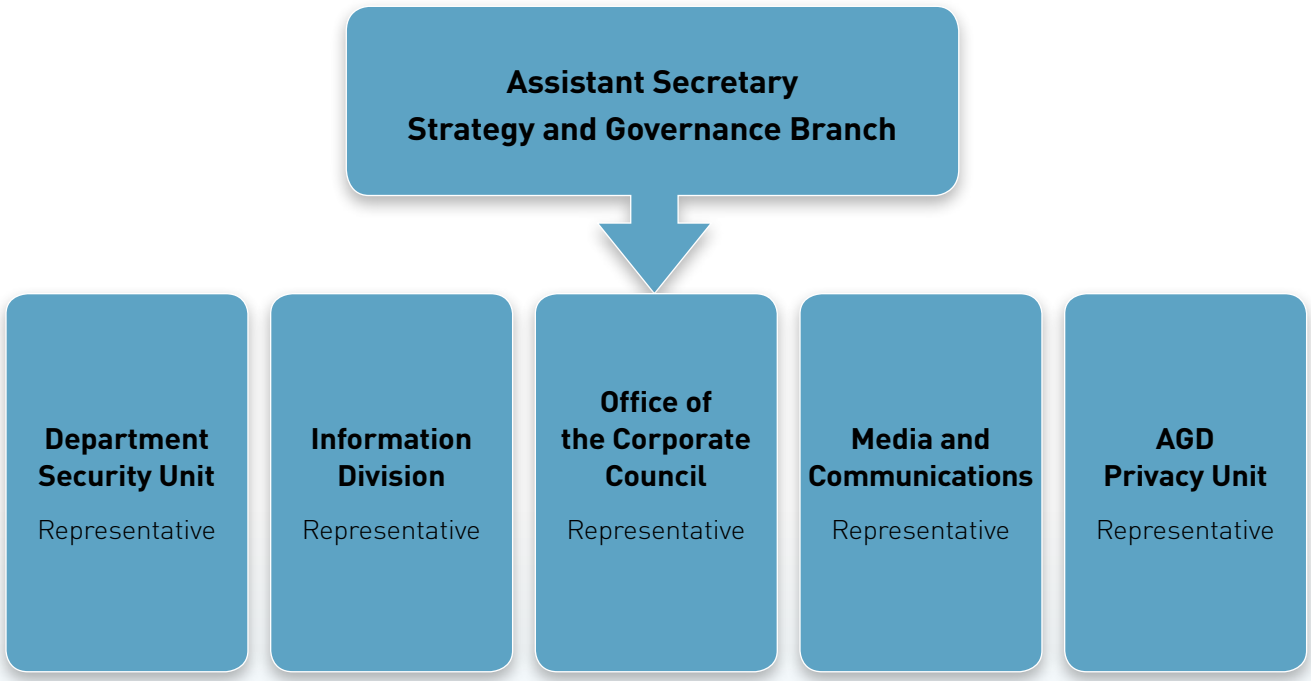
What should the Supervisor or AGD Privacy Unit do?

- Determine whether a data breach has or may have occurred.
- Determine whether the data breach is serious enough to escalate to the Data Breach Response Team (some breaches may be able to be dealt with at the Branch or Section level).
- If so, immediately notify the AGD Privacy mailbox (privacy@ag.gov.au).

Alert the AGD Privacy mailbox (privacy@ag.gov.au) copying the AGD Privacy Officer — Assistant Secretary, Strategy and Governance Branch

AGD Privacy Officer (Assistant Secretary, Strategy and Governance Branch) considers whether a data breach has occurred, and if so, convenes the Data Breach Response Team

Data Breach Response Team



Escalation?

Supervisors (or the AGD Privacy Unit if notified of a data breach by a contractor or third party) should determine whether it is necessary and appropriate to escalate a data breach or suspected data breach to the Data Breach Response Team (Response Team).

Minor Data Breach

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Response Team.

For example, an AGD officer or contractor may accidentally send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be successfully recalled (only relates to internal emails), or if the officer can contact the recipient and obtain an assurance that the recipient has deleted the email, it may not be necessary to escalate the issue to the Response Team.

In deciding whether to escalate a data breach or suspected data breach, supervisors (or the AGD Privacy Unit if notified of a data breach by a contractor or a third party) should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach and what is their relationship to the department?
- Is there (or may there be) a real risk of serious harm to any of the affected individual(s)?
- Has the department been unable to prevent the likely risk of serious harm with remedial action?
- Does the breach or suspected breach indicate a systemic problem in AGD processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If, following consideration of these questions, the supervisor (or the AGD Privacy Unit if data breach is by a contractor or third party) decides the data breach or suspected data breach does not meet any of the above thresholds and considers the breach to be minor, and does not need to be escalated to the Response Team for further action, the supervisor (or the AGD Privacy Unit) should:

- send a brief email to the AGD Privacy inbox that:
    - describes the breach or suspected breach
    - outlines the action taken to address the breach or suspected breach
    - summarises the outcome of that action, and
    - explains why the supervisor considered no further action was required
- save of copy of that email in the following TRIM container:
    - CM reference redacted.

Serious Data Breaches

If the answer to any of the questions above is 'yes', the breach may be an 'eligible data breach'. In such cases, the supervisor (or the AGD Privacy Unit if data breach is by a contractor or third party) must attempt to contact the Assistant Secretary, Strategy and Governance Branch in person or by telephone as soon as possible. If this is not possible, the supervisor (or the AGD Privacy Unit) should immediately attempt to notify another member of the Data Breach Response Team.

The supervisor (or the AGD Privacy Unit if notified of a data breach by a contractor or third party) should follow this up with a written summary of the matter, which includes the information set out above. That summary should be filed in *CM reference redacted.*

Once the Response Team has been notified of a serious and/or eligible data breach, the data breach response process must be followed.

Data Breach Response Process

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks, and using that risk assessment to decide the appropriate course of action. Depending on the nature of the breach, the Response Team may need to include additional staff or external experts, for example an IT specialist/data forensics expert or a human resources adviser.

The key steps when responding to a data breach or suspected data breach are:

- **STEP 1**: Contain
- **STEP 2**: Assess Risk
- **STEP 3**: Breach Notification
- **STEP 4**: Review and Prevent
- **STEP 5**: Post Review Evaluation

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

If possible, the Response Team should undertake steps 1, 2 and 3 simultaneously or in quick succession. At all times, the Response Team should consider whether remedial action can be taken to reduce any potential harm to individuals.

Step 1: Contain

- Notify the Assistant secretary, Strategy and Governance Branch, who may convene the Response Team.
- Immediately contain the breach:
    - alert IT and Building security if necessary, and
    - consider whether DSU and Information Division should be advised.
- Consider whether the Response Team needs other expertise.
- Inform the AGD Executive, including the Secretary, as soon as possible, and provide ongoing updates on key developments.
- Preserve evidence that may be valuable in determining the cause of the breach or allowing AGD to take corrective action.
- Consider a communications or media strategy to manage public expectations and media interest.

Step 2: Assess Risk

- Conduct an initial investigation and collect information about the breach, including:
  - the date, time, duration, and location of the breach
  - the type of personal information involved
  - how the breach was discovered and by whom
  - the cause and extent of the breach
  - a list of affected individuals, or possible affected individuals
  - the risk of serious harm to the affected individuals, and
  - the risk of other types of harm.
- Determine whether the context of the information is important.
- Assess priorities and risks based on what is known.
- Keep records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made.

Step 3: Breach Notification

- Identify the individuals – both internal and external to AGD – whose information may have been compromised.
- Is the breach an 'eligible data breach'? If yes, the breach will trigger NDB scheme requirements.
- In instances where a data breach by the department, a contactor or a third party has triggered notifiable data breach scheme requirements, the Data Breach Response Team will advise senior executive on the nature of the data breach and the process for notifying affected individuals such as:
  - If a contractor or third party experiences a data breach who should notify individuals?
  - how should notification occur? Options include individual emails/SMS messages or notification in a broadly circulated publication.
  - Is there any urgency regarding notification. For example, is there a high level of risk of serious harm, including physical harm, to any of the affected individuals?
- Has the OAIC been notified? OAIC notification is required for eligible data breaches using the OAIC's NDB form.
- Should others, such as the Australian Cyber Security Centre, police/law enforcement, or other agencies or organisations be notified? Notification may be required under contract or MOU, and is highly recommended where other parties may be able to assist in containing the breach or can assist individuals affected by the breach.

Step 4: Review and Prevent

- An investigation should be taken into the cause or causes of the breach.
- Once the factors that contributed to the breach have been identified, a strategy can be developed to address any weaknesses in data handling that contributed to the breach.
- Conduct a post-breach review and provide a report to the AGD Executive on outcomes and recommendations. These could include updates to:
    - departmental physical security
    - departmental records management policies and practices
    - the AGD Data Breach Response Plan
    - other policies and procedures, and
    - staff training and/or practices.
- Consider conducting an audit to avoid future data breaches.

Step 5: Post Breach Evaluation

- Following resolution of a serious data breach, the Response Team should conduct a post-breach evaluation to assess AGD's response to the breach and the effectiveness of this plan and report the results of the evaluation to the AGD Executive.
- The post breach evaluation report should identify and address any deficiencies in this response plan and include recommendations to avoid future data breaches.
- As part of the evaluation, the Response Team should refer to the OAIC's Guide to securing personal information.

Additional Information

The following resources may also be helpful:

- *Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988* (Cth) (OAIC resource)
- AGD Business Continuity Handbook
- AGD Privacy Management Plan
- AGD Protective Security Plan

This Plan is consistent with AGD's Privacy Management Plan, which states that the senior executive is briefed about privacy issues as they occur.

Annual Testing

The Response Team should test this plan with a hypothetical data breach annually to ensure its continued relevance and effectiveness. As with the post-breach evaluation following an actual data breach, the Response Team must report to the AGD Executive on the outcome of each annual test and make any recommendations for improving the plan.

Records Management

Documents created by the Response Team, including post-breach evaluations and annual tests, should be saved in the following Content Manager container:

- CM reference redacted.