Privacy Commissioner
Te Mana Mātāpono Matatapu

OPC Privacy breach response plan

Date: October 2021
Version: 1.0

Contents

Contents

1 Purpose

A privacy breach covered by the Privacy Act 2020 (Part 6) occurs when personal information is lost or subjected to unauthorised access or disclosure, or where an incident prevents OPC from being able to access personal information (either temporarily or permanently). For good privacy practice purposes, this response plan also covers any instances of unauthorised use, modification or interference with personal information held by OPC. Privacy 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.

This response plan is intended to enable OPC to contain, assess and respond to privacy breaches quickly, to help mitigate potential harm to affected individuals and to comply with Part 6(1) of the Privacy Act that commenced on 1 December 2020. Our actions in the first 24 hours after discovering a privacy breach are crucial to the success of our response.

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

OPC experiences privacy breach/privacy breach suspected

- Discovered by OPC staff member, contractor or OPC otherwise alerted

What should the OPC staff member or contractor do?

- Immediately notify your Manager of the suspected privacy breach[1]
- Record and advise your Manager 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 breach

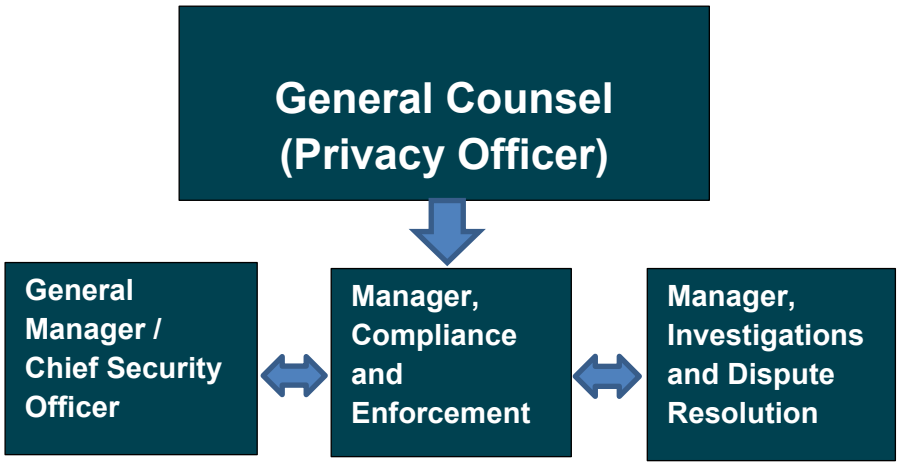
What should the Manager do?

- Determine whether a privacy breach has or may have occurred
- Determine whether the privacy breach is serious enough to escalate to the Privacy Breach Response Team. (Some breaches may be able to be dealt with at the Manager level).
- If so, immediately notify the Privacy Officer

[1] A privacy breach suspected by a member of the Senior Leadership Team or by a Manager may be reported directly to the General Counsel as OPC's Privacy Officer.

Alert the Privacy Officer
• Privacy Officer convenes privacy breach response team

Privacy breach response team — members



When should a privacy breach be escalated to the OPC privacy breach response team?

Managers to use discretion in deciding whether to escalate to the response team

Some privacy breaches may be comparatively minor, and able to be dealt with easily without action from the privacy breach response team (response team).

For example, an OPC staff member may, as a result of human error, 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 staff member can contact the recipient and obtain an assurance that the recipient has deleted the email, it may be that there is no utility in escalating the issue to the response team.

Managers should use their discretion in determining whether a privacy breach or suspected privacy breach requires escalation to the response team. In making that determination, Managers should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to any of the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in OPC processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then the Manager should attempt immediate verbal contact with the Privacy Officer, or if this is not possible, another primary response team member.

The checklist below sets out the steps that the response team will take in the event of a serious privacy breach.

Managers should inform the Privacy Officer of minor breaches or near misses

If a Manager decides not to escalate a minor privacy breach or suspected privacy breach to the response team for further action, the Manager should:

- send a brief email to the General Counsel (OPC's Privacy Officer) and to the General Manager that contains the following information:
    - description of the breach or suspected breach or "near miss"
    - action taken by the Manager or staff member to address the breach or suspected breach
- the outcome of that action, and
- the Manager's reasons for their view that no further action is required
- save of copy of that email in the following location:
    - Privacy Breach Response – reports and investigation of privacy breaches within OPC

OPC privacy breach response process

There is no single method of responding to a privacy breach. Privacy breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, 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.

There are four key steps to consider when responding to a breach or suspected breach.

Step 1: Contain the breach
Step 2: Assess the risks associated with the breach
Step 3: Consider breach notification
Step 4: Review the incident and take action to prevent future breaches

The response team should ideally undertake steps 1, 2 and 3 either 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.

The response team should refer to the checklist below. and to OPC's guidance on responding to privacy breaches which provides further detail on each step.

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.

Following serious privacy breaches, the response team should conduct a post-breach review to assess OPC's response to the breach and the effectiveness of this plan and report the results of the review to the OPC Senior Leadership Team. The post-breach review report should identify any weaknesses in this response plan and include recommendations for revisions or staff training as needed.

The response team should also consider the following documents where applicable:

- OPC Business Continuity Plan
- ICT Incident Response Plan
- ICT Disaster Recovery plan

Testing this plan

Members of the response team should test this plan with a hypothetical privacy breach annually to ensure that it is effective. As with the post-breach review following an actual privacy breach, the response team must report to the OPC Senior Leadership Team on the outcome of the test and make any recommendations for improving the plan.

Records management

Documents created by the response team, including post-breach and testing reviews, should be saved in the following location:

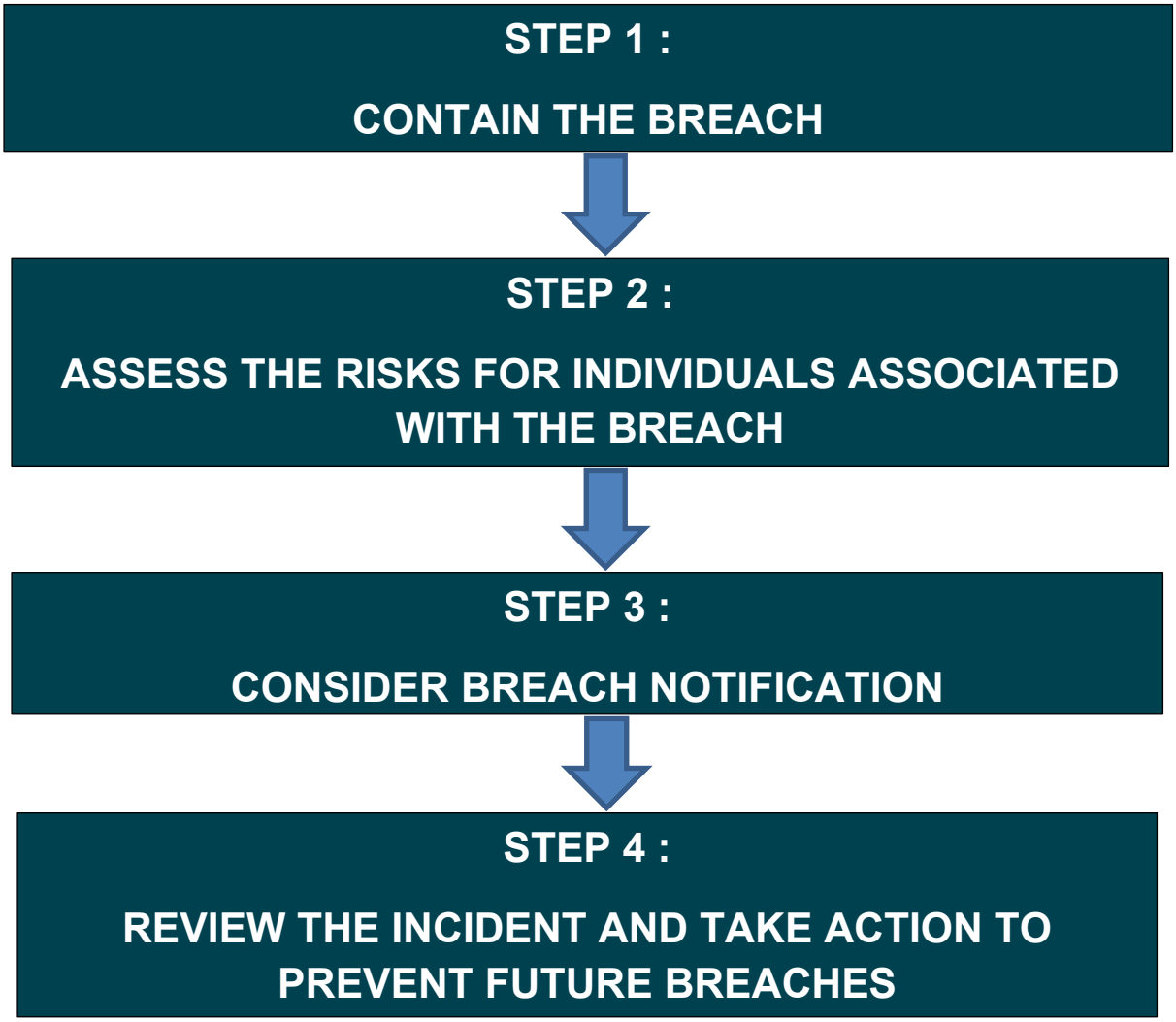
- Privacy Breach Response – reports and investigation of privacy breaches within OPC

Reporting

OPC's privacy management plan states that the internal handling of personal information will be an agenda item on the Senior Leadership Team meetings at least once each quarter and include a report of any privacy complaints against OPC and internal privacy breaches.

The General Manager should liaise with the Privacy Officer on the preparation of reports on internal privacy breaches.

OPC's Privacy Breach Response Check List



Step 1: Contain the breach

- Notify the General Counsel (OPC's Privacy Officer), who may convene the privacy breach response team.

- Immediately contain breach:
  - IT to implement the ICT Incident Response Plan if necessary.
  - Building security to be alerted if necessary.
  - Consider whether Objective systems administrator needs to be advised.

- Consider whether team needs other expertise.

- Inform the OPC Senior Leadership Team, including the Privacy Commissioner, as soon as possible; provide ongoing updates on key developments.

- Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing OPC to take appropriate corrective action.

- Consider a communications or media strategy to manage public expectations and media interest.

Step 2: Assess the risks for individuals associated with the breach

- Conduct initial investigation, and collect information about the breach promptly, including:
    - the date, time, duration, and location of the breach
    - the type of personal information involved in the breach
    - how the breach was discovered and by whom
    - the cause and extent of the breach
    - a list of the affected individuals, or possible affected individuals
    - the risk of serious harm to the affected individuals
    - the risk of other harms.

- Determine whether the context of the information is important.

- Establish the cause and extent of the breach.

- Assess priorities and risks based on what is known.

- Keep appropriate 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: Consider breach notification

- Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.

- Determine whether and how to notify affected individuals. Does the breach trigger the notification requirements of Part 6(1) of the Privacy Act 2020 – is the breach likely to result in serious harm to any of the individuals to whom the information relates and OPC has not been able to prevent the likely risk of serious harm through remedial action. In some cases, it may be appropriate to notify the affected individuals immediately, e.g., where there is a high level of risk of serious harm to affected individuals. If the notification threshold is triggered – a formal notification to the Privacy Commissioner through OPC's Notify Us form should be completed and registered in Objective. Even if the notification threshold is not met would notifying the individuals be appropriate?

- Consider whether others should be notified, including CERT, police/law enforcement, or other agencies or organisations affected by the breach or can assist in containing the breach or assisting individuals affected by the breach, or where the OPC is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.

- Plan for OPC's reporting obligations to the Minister (under "no surprises" and the 3 monthly report) and to Parliament (in the annual report)

Step 4: Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach.
- Implement a strategy to identify and address any weaknesses in data handling that contributed to the breach.
- Conduct a post-breach review and report to the OPC Senior Leadership Team on outcomes and recommendations:
    - Update security and response plan if necessary.
    - Make appropriate changes to policies and procedures if necessary.
    - Revise staff training practices if necessary.
    - Consider the option of an audit to ensure necessary outcomes are affected.

RESPONSIBILITIES	
Persons/ Areas Affected	ALL OPC Staff & Contractors
Contact	General Manager /General Counsel
Approval Authority	Privacy Commissioner
Last Review Date	October 2021