SIMPSON GRIERSON

# Notifiable Privacy Breaches

If your business is subject to the 2020 Privacy Act, it is mandatory to report a notifiable privacy breach to the Privacy Commissioner and affected individuals. This guide can be used to determine whether there is a notifiable privacy breach, and how to notify.

## Do you need to notify?

A privacy breach is notifiable if it is reasonable to believe it has caused, or is likely to cause, serious harm to an affected individual. Your assessment should cover the following three questions:

### 1. Has there been a privacy breach?

- Has there been unauthorised access, disclosure, alteration, loss, or destruction of personal information?
- Has there been an action that prevents access to personal information on either a temporary or a permanent basis?

If **YES** to either question, there has been a privacy

### 2. Has the privacy breach caused, or is it likely to cause, harm?

Has the privacy breach caused, or is it likely to cause:

- Financial loss, loss of employment, physical injury or other forms of specific damage to an individual?
- Any adverse effect on the rights, benefits, privileges, obligation or interests of an individual?
- Significant humiliation, significant loss of dignity or significant injury to feelings?

If **YES** to any question, the breach has caused, or is likely to cause, harm

### 3. Is the harm serious?

Consider the following relevant factors:

- Is the personal information sensitive in nature?
- Has any action been taken to reduce the risk of harm?
- What is the nature of the harm that may be caused?
- Who has or may obtain the personal information as a result of the breach?
- Is the information protected by a security measure?
- Are there any other relevant matters, eg:
  - Is there risk of further circulation?
  - How long has the information been exposed?
  - Did the breach involve theft or a cyber-attack?
  - Is there evidence of malicious intent?
  - Has the information been recovered?

If **YES**, the breach is likely to be a notifiable privacy breach

SIMPSON GRIERSON

# Steps to take if there is a notifiable privacy breach

If you have a notifiable privacy breach, then you need to notify the Privacy Commissioner and affected individuals (or give public notice), as soon as practicable. Your notification should cover the following points:

## Notice to Privacy Commissioner

- ✓ Description of breach, including number of affected individuals (if known), and identity of person/body agency suspects may be in possession of information as a result of the breach;
- ✓ Explain any steps taken, or any intended steps, and whether the affected individuals has been or will be contacted;
- ✓ If applicable, state the reasons for giving public notice, or relying on any exception/notification delay;
- ✓ Provide the names of any other agencies contacted about the breach and the reasons for having done so; and
- ✓ Provide details of a contact person within your agency for inquiries.

## Notice to affected individual or individuals

- ✓ Description of the breach, including whether any recipients, or suspected recipients, have been identified. You should NOT provide any personal information about any other individual;
- ✓ Explain any steps taken, or any intended steps, in response to the breach;
- ✓ Where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any);
- ✓ Confirm the Privacy Commissioner has been notified;
- ✓ Advise that the individual has the right to complain to the Privacy Commissioner; and
- ✓ Provide details of a contact person within your agency for inquiries.

Note that there are occasions where you will NOT need to notify individuals. These include if the individual is under the age of 16, or if notification would be likely to prejudice an individuals' health. A full list of exceptions can be found in section 120 of the Privacy Act 2020.

You may delay notification to individuals if you believe notification or public notice may have risks for the security of personal information, and these risks outweigh the benefits of informing individuals.

**Public Notification**

If it is not reasonably practicable to notify an individual, you will instead have to give public notice of the privacy breach.

Take care not to inadvertently breach any Information Privacy Principles when describing a notifiable privacy breach to an affected individual.

If you have any questions, please contact your usual Simpson Grierson advisor, or one of our privacy specialists:

## Contacts


**Jania Baigent, Partner**
M: 021 550 554
E: jania.baigent@simpsongrierson.com

**Karen Ngan, Partner**
M: 021 648 977
E: karen.ngan@simpsongrierson.com

**Sally McKechnie, Partner**
M: 021 180 7236
E: sally.mckechnie@simpsongrierson.com