# NZ NOTIFIABLE PRIVACY BREACH FACTSHEET

A notifiable privacy breach (**NPB**) occurs when personal information maintained by your organisation is lost, accessed, or disclosed without authorisation, and this breach is likely to cause serious harm. The *Privacy Act 2020* requires organisations to report these breaches to the Office of the Privacy Commissioner (**OPC**) and, in most cases, to affected individuals.

This factsheet explains what a privacy breach is, your reporting obligations, and how to limit an NPB's impact.

## 1, WHEN IS A BREACH NOTIFIABLE?

A breach is notifiable if it meets the following criteria:

- personal information is lost, or there is unauthorised access or disclosure;
- the breach is likely to cause serious harm; and
- your organisation is unable to prevent this harm.

A breach may not be notifiable if the harm is not serious or if steps can be implemented to reduce its impact.

## 2. WHAT IS CONSIDERED SERIOUS HARM?

Serious harm can include:

- physical harm or intimidation;
- financial fraud (e.g., unauthorised credit card transactions);
- family violence; or
- psychological or emotional harm.

Whether a data breach could result in "serious harm" depends on the perspective of a "reasonable person". It considers several factors, including:

- sensitivity of the information;
- who has obtained or may obtain the information;
- whether the information is protected by security measures; and
- the nature of potential or actual harm.

The OPC has a helpful self-assessment tool, 'NotifyUs', which allows you to determine if a privacy breach is likely to cause serious harm and whether it is or is not notifiable.

## 3. WHAT ARE MY REPORTING OBLIGATIONS?

If you experience a notifiable privacy breach:

- report to the OPC as soon as possible (expected within 72 hours) using the NotifyUs online tool; and
- notify affected individuals, unless an exception applies.

Failure to report notifiable privacy breaches may result in fines of up to $10,000.

Notification to impacted individuals should:

- summarise the events of the breach;
- outline the potential impact; and
- detail the actions you are taking to mitigate any risks.

## 4. HOW CAN I LIMIT THE IMPACT OF A DATA BREACH?

You can limit the impact of a breach by implementing a Data Breach Response Plan. Your plan should set out:

- who in the business is responsible for dealing with the breach; and
- what actions they must take if a breach occurs.

If a breach occurs, you can limit its impact by:

- acting immediately to stop the breach and to prevent further unauthorised access or disclosure;
- recovering lost records;
- remotely deleting files;
- shutting down the system that resulted in the breach; and
- removing certain individuals' access to the system.


## CONTACT US

visit our website | **legalvision.co.nz**
email us | **info@legalvision.co.nz**
call us | **0800 005 570**