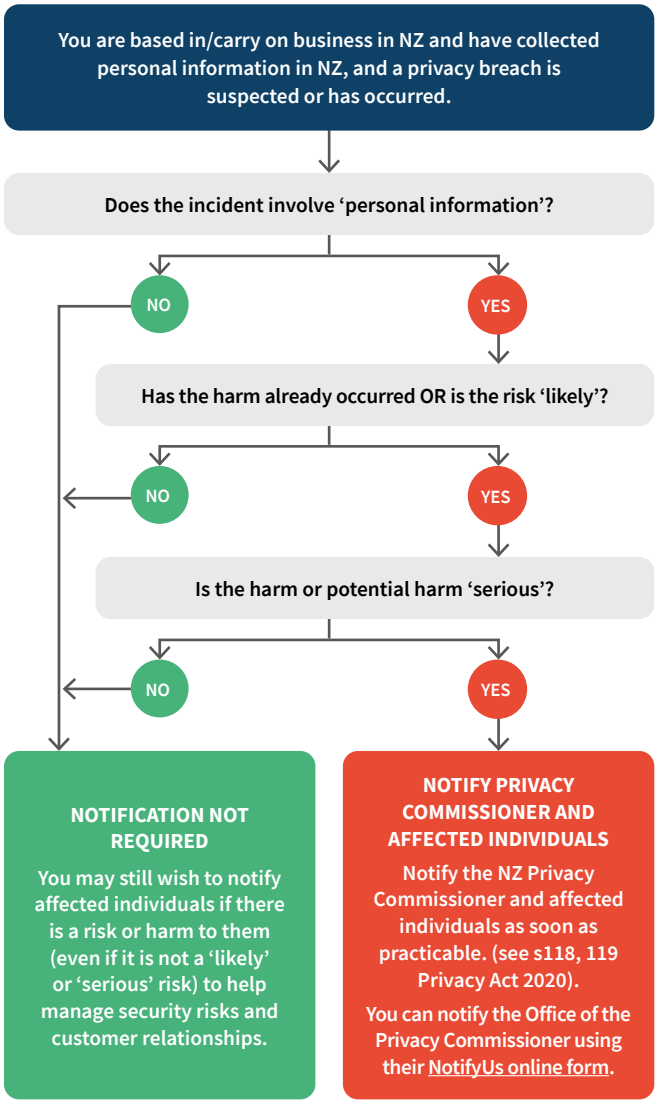
ARTICLE

New Zealand's data breach laws have international implications

From 1 December 2020, New Zealand's mandatory data breach notification laws take effect. If your organisation carries on business or is based in New Zealand, and you experience a data breach, you may be required to notify the regulator and affected individuals. If you don't comply, you may face fines or other regulator action.

This is a brief snapshot of how you determine if you need to notify.



KEY TERMS

What is a 'privacy breach'?

A privacy breach (commonly called a 'data breach') is the unauthorised or accidental access to, or disclosure, alteration, loss or destruction of personal information held by an 'agency' - any organisation or business, whether in the public sector or private sector. This includes government departments, companies and businesses, social clubs and other types of organisations.

A privacy breach also occurs when any action prevents a person from accessing their personal information that is held by an agency – for example, ransomware or denial of service attacks - s112 *Privacy Act 2020*.

What is 'personal information'?

Personal information is "information about an identifiable individual" – s7 *Privacy Act 2020*.

The information does not need to name someone specifically to be personal, if they are identifiable in other ways, for example, through their home address.

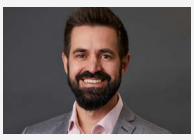
How to assess 'likely risk of serious harm'?

When assessing the likelihood and severity of the privacy breach, you must consider:

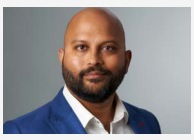
- if you have been able to take action to reduce the risk of harm following the breach (for example, whether the personal information has been recovered, or if user account passwords have been reissued)
- if the personal information is sensitive in nature (for example, health or genetic information, unique identifiers like a passport or driver's licence, or credit card and account numbers)
- what kind of harm may be caused to affected individuals (for example, discrimination, emotional, employment, financial, physical or reputational harms, loss of access or opportunity, increased risk of identity theft)
- who has obtained or may obtain personal information as a result of the breach (if known – for example, if personal information has been accessed by criminal actors)
- if the personal information is protected by a security measure (such as encryption).

(s113 *Privacy Act 2020*)

We can help you improve your data breach readiness, or support you in managing a data breach.



CHRISTOPHER HATFIELD
Managing Director
+61 (0) 437 373 130
christopher.hatfield@fticonsulting.com



TIM DE SOUSA
Senior Director
+61 (0) 413 248 107
tim.desousa@fticonsulting.com

MIN CAI
Senior Director
+61 (0) 450 484 207
min.cai@fticonsulting.com