Privacy Commissioner
Te Mana Mātāpono Matatapu

Ask the experts: what you need to know about notifying individuals about a privacy breach

Susan Allen, Compliance and Enforcement Manager

Vinka Cisternas-Torres, Senior Compliance Officer

Privacy Week 2024
Busting privacy myths!
13-17 May
www.privacy.org.nz
Privacy Commissioner
Te Mana Mātāpono Matatapu

What are the notification requirements?

Relevant sections of the Privacy Act 2020:

- "An agency must notify an affected individual as soon as practicable after becoming aware that a notifiable privacy breach has occurred" – **section 115**
- "Exceptions to or delay in complying with requirement to notify affected individuals or give public notice of notifiable privacy breach" – **section 116**
- "Requirements for notification" – **section 117**
- Assessment of a breach as being 'notifiable' **– section 113**

Why do I need to notify?

Section 115 notifying individuals or give public notice

"An agency must notify an affected individual as soon as practicable after becoming aware that a notifiable privacy breach has occurred"

- 'As soon as practicable' – what does this mean?
- 'Becoming aware' – means having a degree of knowledge or an assessment about the risk of harm from the privacy breach.

What to notify?

Section 117 requirements for notification

- Describe what happened - what information was disclosed and what hasn't been disclosed
- Where their information has gone and who might be in possession it
- What you're doing to control or reduce the harm – containing the breach
- What support you can offer to help people protect themselves and what steps the affected people can take to protect themselves
- Make sure they know their right to make a complaint to OPC and provide information on how to do that
- Give them a contact at your organisation if they have questions or want to make a complaint
- Confirm that you've notified OPC

Do I always need to notify?

Section 116 exceptions or delay for:

- Prejudice the security, defence, or international relations of New Zealand
- Prejudice the maintenance of the law by a public sector agency
- Endanger someone's safety
- Reveal a trade secret
- Notifying a representative – child or vulnerable person
- Notifying by public notice
- Delaying notification

Busting some myths about notifying

- “They already know about the breach because they told us!”
- “It’s part of an HR investigation so I can’t say anything until that’s finished”
- “The affected individual isn’t concerned about the breach so it’s not serious”
- “I’m pretty sure I know where the lost papers are so I’m sure it’s ok”
- “The breach was a long time ago so it’s no longer relevant”

When it goes right (and wrong)

Case study one

- Small business subject to phishing attack
- Clients weren't notified and customer lost $150,000
- Business found to be in breach of Information Privacy Principle 5 (information security) and the section 115 and 117 notification requirements

Case study two

- Financial services provider subject to cyber attack
- The agency assessment determined it was highly likely the threat actor exfiltrated personal information
- Steps were taken to inform through media their systems were compromised and advised customers to be cautious. Regular updates were provided through the course of the investigation.

He pātai?
Any questions?