Client Update

JULY 2021

wotton kearney

A founding member of LEGALIGN GLOBAL

# OPC gets tough on mandatory privacy breach notification

## AT A GLANCE

- The Privacy Act 2020 introduced requirements for mandatory notification of serious privacy breaches.[1]
- Just over six months after it became law, the Office of the Privacy Commissioner (**OPC**) has released further guidance on mandatory notification in a blog post.
- The update makes it clear the OPC has ended the grace period for agencies to adapt to the new rules.
- The new guidance also sets out a more rigorous approach to notifying privacy breaches and emphasises that the OPC will consider prosecuting organisations that commit breaches.

## THE NEW GUIDANCE

The Privacy Act 2020 introduced mandatory notification for "serious" privacy breaches. A privacy breach includes "unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information" and "an action that prevents the agency from accessing the information on either a temporary or permanent basis". Notification of a "privacy breach" is necessary "as soon as practicable" where the breach is likely to cause "serious harm" to an individual.

In its post, *OPC send warnings to organisations to get it right next time*, the Office of the Privacy Commissioner (**OPC**) states it is "taking a more proactive approach to remind and warn individual organisations of their statutory responsibilities under the Privacy Act 2020."

The guidance note goes on to set out a more rigorous approach to notifying privacy breaches. This includes:

- requiring notification within 72 hours of a breach being detected
- reiterating that notification is required for loss of personal information, but also denial of access to personal information, and
- emphasising that the OPC will consider prosecuting organisations that commit breaches.

[1] We summarised the key components of the new regime in our last set of updates here.

In its guidance note, the OPC expressed dissatisfaction with agencies' present approach to notification. While acknowledging that "the Act is silent on precise timing", the OPC has clarified that notifying privacy breaches "as soon as practicable after becoming aware" means within 72 hours.

The post also clarifies that ransomware attacks rendering information inaccessible can constitute privacy breaches. It goes on to highlight three examples of poorly managed breaches concerning an ex-employee, an erroneous physical mail-out, and what it describes as a "serious privacy breach".

The update ends with an explicit word of warning, particularly around timing

> *"It has now been six months since the Privacy Act 2020 took effect. The law has changed. Mandatory privacy breach reporting means telling our Office as soon as practicable if there's been a serious privacy breach. It doesn't mean telling us after the dust has settled. It means telling us sooner rather than later. Otherwise, there are potential consequences because the Privacy Act has given our Office new powers to enforce the law change."*

## THE KEY ISSUES FOR INSURERS, BROKERS AND THEIR CUSTOMERS

The OPC's update reflects a shift in its approach to privacy breach notification. The message is now clear: the grace period for agencies to adapt to the new rules is over.

***"As soon as practicable" = 72 hours***

The guidance note clarifies breaches should be notified within 72 hours unless there are "extenuating circumstances". While the 72 hour period aligns with the timing referred to in the EU's GDPR, it raises some practical questions for application in New Zealand.

The Privacy Act requires notification where it is reasonable to believe the breach is likely to cause serious harm to individuals. In its guidance, the OPC states that agencies should notify during the rectification process, rather than after the fact. How this will work in practice remains to be seen as it takes time following an incident to determine what has occurred, the information affected, and what impact this may have on individuals. For example, it often takes a forensic provider some time to identify that information has been exfiltrated after a ransomware attack.

The OPC's guidance suggests that agencies should notify when there may be a risk of serious harm – although that is a lower threshold than required by the strict wording of the Privacy Act (when serious harm is "likely"). If this is the new approach organisations will need to consider notifying early, which will also mean risk assessments need to be conducted quickly.

***Prevention of access and ransomware are on the OPC's radar***

When assessing privacy breaches, the OPC has emphasised that organisations must consider both access and disclosure of information and prevention of access issues. This highlights the importance of putting individuals at the heart of any risk assessment.

Agencies should be concerned about both data exfiltration and ransomware encryption that prevents access to impacted personal information. This is particularly pertinent for incidents involving ransomware, which are addressed specifically in the update.

> **The shift in its [the OPC] approach to the privacy breach notification is clear - the grace period for agencies to adapt to the new rules is over.**

***Get breach counsel involved early***

The new guidance makes it clear that OPC expects to be quickly informed of a wide range of incidents. This makes it increasingly important for agencies to get legal advice about their privacy and notification obligations early in an incident. An approach of ignoring legal and privacy issues until after systems are restored may leave organisations exposed.

There is also significant benefit in engaging with breach counsel ahead of an incident. The OPC's update emphasises its expectation that organisations will adopt, follow and update incident response plans. The case studies also flag the OPC's intention to punish agencies that make the same error multiple times. Breach counsel can help prepare and implement incident response plans and review prior incidents to ensure that key risks are mitigated.

> **It is important for agencies to get legal advice about their privacy and notification obligations early in an incident.**

wotton kearney

## Need to know more?

If you would like to know more about implementing an incident response plan, reviewing a previous incident, or understanding your obligations under the Privacy Act 2020, get in touch with a member of our cyber and data risks team.

**Mark Anderson**
Partner & NZ Cyber Leader (Auckland)
T: +64 9 280 0524
E: mark.anderson@wottonkearney.com

**Joseph Fitzgerald**
Special Counsel (Wellington)
T: +64 4 260 4796
E: joseph.fitzgerald@wottonkearney.com