NZ Privacy Act 2020

UPDATE 3 – DECEMBER 2020

wotton kearney

A founding member of LEGALIGN GLOBAL

The new *Privacy Act 2020* came into effect on 1 December 2020. The Act introduces a range of reforms that bring New Zealand into line with international best practice for privacy and data protection. The reforms include mandatory notification requirements and extra-territorial jurisdictional scope.

AT A GLANCE:

- On 1 December 2020, New Zealand's new *Privacy Act 2020* came into effect.
- Arguably the most important change created by the Act is that it will now be mandatory for organisations to report privacy breaches in situations likely to cause serious harm to the individual concerned.
- Organisations will now have to decide whether they have a reasonable belief that any breach has caused serious harm.
- This is a critical evaluation following an incident and carries real reputational, legal and financial risk to an organisation.

The serious 'serious harm' assessment

Arguably the most dramatic impact of the Act is the mandatory requirement for organisations to report privacy breaches to the Privacy Commissioner and those affected in certain situations.

The nature of privacy breaches can be varied and sometimes complex. Where the breach is the result of an external cyber-attack, expert input is often required to identify the point of attack, what information has been taken, how long the 'attacker' has been in the system, and whether there is a credible threat to the information being disclosed. And expert consideration of the risks in notifying or not notifying need to be considered.

Organisations will now have to decide whether they have a reasonable belief that a breach has caused serious harm. This decision is time-critical – as is the decision to notify. Notification is required as soon as it is reasonably practicable to do so, even if the full extent of the privacy breach is unknown. Getting this time-sensitive decision right is now reputationally and legally critical. It is also financially important, given the potential penalty of $10,000 for failure to notify without a reasonable excuse.

HAS A BREACH OCCURRED?

In assessing whether there is a need to notify, the first thing to assess is whether the organisation has a reasonable belief that a privacy breach has occurred.

In a typical ransomware attack, ransom notes are often a tell-tale sign that a privacy breach has occurred. However, sometimes attackers can leave without a trace and organisations can be left relying on a 'gut-feeling' that something is not right. In those circumstances, IT assistance can be invaluable in helping to establish whether there has been a breach and to identify its extent.

WHAT IS SERIOUS HARM?

After determining that there has been a breach, the next thing to consider is whether the breach has caused, or is likely to cause, serious harm to individuals.

The Act does not provide a definition of what 'serious harm' is. 'Reasonable belief' about what may cause serious harm requires an understanding of the extent of the privacy breach and its impact. While this can be difficult without expert assistance, there are common factors to consider, including assessing:

- the nature of the information lost, including whether the information held is personal/sensitive
- where the information has gone due to the privacy breach (e.g. Was it a malicious hacker?)
- the nature of the harm caused to people affected by the breach, which may involve consideration of discriminatory, identity, reputational, emotional, financial or loss of information factors
- the likelihood that the harm will significantly affect an individual or individuals
- the steps taken to reduce the harm, and
- the security measures in place to protect the information from being accessed.

ASSESSING SERIOUS HARM – EXAMPLE 1

Let's suppose that a local bakery suffers a ransomware attack. The unknown attackers have left a ransomware note threatening to release recipes used by supermarkets unless a $50,000 payment is made. There is no evidence that any other information was accessed or taken. In this case, there is a clear privacy breach.

Assessing whether this privacy breach will cause serious harm requires more analysis, including considering:

- the nature of the information stored by the bakery, which is, generally, not relating to individuals and so non-sensitive
- the potential reputational harm, which in this case is assessed as being low, and
- whether the bakery was taking proactive steps to protect the information from being accessed, which in this case it was.

In this example, the privacy breach is unlikely to cause 'serious harm' to an affected individual (as it does not involve personal information) so it would not require notification. However, even a bakery may hold sensitive data (for example, employee's financial/employment or health records) and so even for such a small business, understanding the type of data at risk is critical.

> **Organisation will now have to decide whether they have a reasonable belief that a breach has caused serious harm. This decision is time-critical – as is the decision to notify.**

ASSESSING SERIOUS HARM – EXAMPLE 2

In our second example, a large medical clinic has been subjected to a SIM swapping attack. As with our bakery example, the unknown attackers have left a ransomware note threatening to release information unless a $50,000 payment is made. In this case, there is a clear privacy breach. Medical records are at risk.

However, in this example, serious harm may be likely as:

- the compromised data includes personal and sensitive information critical to individuals
- the potential harm caused to individuals could include reputational, emotional and physical damage, and would also affect the therapeutic relationship between the affected individuals and medical practitioners, and
- there were no barriers to prevent the attacker getting access to the information.

In this example, the privacy breach would need to be notified to the Privacy Commissioner and to those affected. Careful consideration of the mode, timing, and method for delivering the notification to affected individuals is needed, and an expert panel (legal/crisis management/IT forensic and technical) is invaluable in such a time of crisis.

MANAGING THE RISKS WITH A BREACH RESPONSE PLAN

While our two examples show how the criteria can be applied, each 'serious harm' decision will turn on the specific nature of the information held by an organisation and will require a careful analysis.

Given the time-sensitive nature of this decision, and the associated reputational, legal and financial risks, organisations should have a breach response plan in place. Depending on the scale of the organisation, this plan should detail – among other things – the 'serious harm' issues to consider, a list of external providers, the information that needs to be collected, timeframes for responding, and the individuals at the organisation who are responsible for making the decision to notify.

wotton kearney

Need to know more?

For more information or assistance in a breach response plan, please contact our authors.

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

Joseph Fitzgerlad
Senior Associate
T: +64 4 260 4796
joseph.fitzgerald@wottonkearney.com

Sierra Ryland
Senior Associate
T: +64 4 974 9280
sierra.ryland@wottonkearney.com

David Smith
Solicitor
T: +64 9 377 1881
david.smith@wottonkearney.com