Privacy law changes

BY ANDREW SKINNER

NEW PRIVACY LAWS, WHICH WILL REPLACE THE CURRENT PRIVACY ACT, ARE EXPECTED TO COME INTO FORCE IN 2020. THE PURPOSE OF THE NEW LAW IS TO PROMOTE AND PROTECT INDIVIDUAL PRIVACY. THE NEW LAWS WILL MAINTAIN THE CURRENT INFORMATION PRINCIPLES BASED FRAMEWORK WHILE UPDATING THE LAW TO REFLECT THE NEEDS OF THE DIGITAL AGE.

Unfortunately, serious privacy breaches continue to occur on a relatively frequent basis and often make headlines damaging the reputation of the agency involved. Two recent examples reported in August highlight the risks of not appropriately protecting personal information:

- the Ministry for Culture and Heritage revealed that around 300 people had had their personal documents compromised following an error on a Ministry commissioned website
- a receptionist from a medical centre disclosed personal information about patients of the centre at a social gathering

KEY CHANGES

As currently drafted, the new law does not substantially change the information privacy principles regarding the collection, storage, disclosure and use of personal information. However, the new law significantly increases the powers of the Privacy Commissioner and the key changes are:

- the mandatory reporting of certain privacy breaches
- the power of the Privacy Commissioner to issue compliance notices
- the introduction of new criminal offences
- the power of the Privacy Commissioner to make binding decisions on information access requests
- the strengthening of the Privacy Commissioner's information gathering powers

MANDATORY REPORTING

Probably the most significant change under the new law is the introduction of a mandatory notification regime for certain privacy breaches. An agency must disclose a privacy breach to the Privacy Commissioner when it is reasonable to believe that the breach has caused serious harm to an affected individual or individuals or is likely to do so. In deciding whether a privacy breach is likely to cause serious harm an agency must consider certain factors, including any actions taken by the agency to reduce the risk of harm following the breach, whether the personal information is sensitive, the nature of the harm that may be caused, who has had access to the personal information and whether the personal information is protected by a security measure. There will be certain exceptions to the mandatory notification provisions such as where notification may endanger the safety of any person or reveal a trade secret. It is an offence for an agency to fail to notify the Privacy Commissioner of a notifiable privacy breach and the agency may be liable on conviction to a fine not exceeding $10,000.00.

WHAT SHOULD YOU DO TO PREPARE?

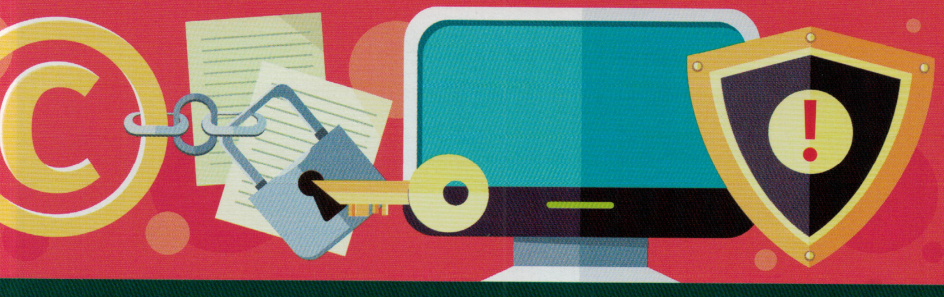
The law changes present an opportunity for businesses to review their processes for handling personal information to ensure that the correct processes are in place and the requirements understood. Whilst the maximum fine is relatively modest, the reputational damage from a privacy breach will be no doubt be of serious concern to companies.

Prior to the introduction of the new law, businesses in the building and construction industry need to review the personal information they collect, such as:

- personal details of customers (which may include the credit information of customers to the extent credit checks are carried out prior to commencing building work)
- employee information
- information relating to health and safety incidents

Having reviewed the personal information collected, the business then needs to confirm what happens to that information, who has access to it and how it is used. Other policies also need to be considered such as how to deal with requests to correct information. Many businesses now display a privacy policy or statement on their website which clearly explains how the business handles personal information. Once this review has been completed the business should provide training on the privacy rules to staff prior to the new law commencing to ensure that everyone understands the importance of protecting the personal information of individuals arising out of the activities of the business.

This article is intended to provide general guidance and does not constitute legal advice, which may vary depending on your circumstances.





Andrew Skinner is formerly General Counsel at CARTERS and is a Partner at Stewart Germann Law Office
Email: andrew@germann.co.nz