Privacy Act 2020 and mandatory privacy breach reporting…
Under the Privacy Act 1993, although encouraged as best practice, agencies (which includes Lions Clubs and Lions Charitable Trusts) did not in the past have to report a privacy breach.

The Privacy Act 2020, which came into force on 01 December 2020, will make reporting of privacy breaches mandatory, if they classify as a "notifiable privacy breach" and this will apply to Not For Profits and Charities.

What is a privacy breach?

The new Act provides two interpretations of what a privacy breach is, in relation to personal information held by an organisation (agency). These include:

· unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or

· an action that prevents the agency from accessing the information on either a temporary or permanent basis;

The first meanings is what is commonly understood to be a privacy breach. This includes incidents such as unauthorised access to a system, losing devices such as laptops or USBs that contain personal information, or accidentally disclosing personal information to the wrong person.

The second meaning encompasses incidents such as ransomware attacks. This form of cyberattack has become increasingly common in recent years.

In a ransomware attack, an outside user gains access to systems or databases, and either locks the users out or encrypts their files. Often the hacker will subsequently demand a financial payment in return for restoring access or providing a key to decrypt files. There have been several incidents where organisations have refused to make payment, and sensitive information has been deleted or released to the public.

When is a breach notifiable?

A privacy breach is notifiable when it is reasonable to believe the breach has caused, or is likely to cause, serious harm to the affected individual(s). The Act provides several factors that an agency must consider when deciding if a breach is notifiable:

· any action taken by the agency to reduce the risk of harm following the breach;

· whether the personal information is sensitive in nature;

· the nature of the harm that may be caused to affected individuals;

· the person or body that has obtained or may obtain personal information as a result of the breach (if known);

· whether the personal information is protected by a security measure; and

· any other relevant matters.

It is important to note that the breach is notifiable when it is reasonable to believe the breach has, or is likely to cause, serious harm. If or when the belief is "reasonable" is a matter for

the organisation to determine. Organisations need to understand that a failure to notify the Commissioner of the breach, where reasonable belief exists, is an offence punishable with a fine of up to $10,000.

Who must the breach be reported to?

If the breach is notifiable, it must be reported to the Privacy Commissioner and the affected individual. The agency must notify the affected individual as soon as reasonably practicable after becoming aware that a notifiable breach has occurred (unless an exception applies).

The Act provides a detailed list of requirements that must be included in a notification to the Commissioner or affected individual.

A notification to the Commissioner from an organisation must—

(a) describe the privacy breach, including—

(i) the number of affected individuals (if known); and

(ii) the identity of any person or body that the organisation suspects may be in possession of personal information as a result of the privacy breach (if known); and

(b) explain the steps that the agency has taken or intends to take in response to the privacy breach, including whether any affected individual has been or will be contacted; and

(c) if the agency is intending to give public notice of the breach, set out the reasons justifying that action (this can only be done in special circumstances set out in the Act); and

(d) if the agency is relying on an exception, or is delaying notifying an affected individual or giving public notice, state the exception relied on and set out the reasons for relying on it or state the reasons why a delay is needed and the expected period of delay; and

(e) state the names or give a general description of any other agencies that the organisation has contacted about the privacy breach and the reasons for having done so; and

(f) give details of a contact person within the organisation for inquiries.

A notification to an affected individual or a representative must—

(a) describe the notifiable privacy breach and state whether the organisation has or has not identified any person or body that the agency suspects may be in possession of the affected individual’s personal information (but, must not include any particulars that could identify that person or body , unless certain exceptions apply); and

(b) explain the steps taken or intended to be taken by the organisation in response to the privacy breach; and

(c) where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any); and

(d) confirm that the Commissioner has been notified; and

(e) state that the individual has the right to make a complaint to the Commissioner; and

(f) give details of a contact person within the organisation for inquiries.

A notification to an affected individual may identify a person or body that has obtained or may obtain that affected individual's personal information (where the identity is known) if the organisation believes on reasonable grounds that identification is necessary to prevent or lessen a serious threat to the life or health of the affected individual or another individual.

A notification to an affected individual must not include any particulars about any other affected individuals.

Notification must be made as soon as practicable, but may be provided incrementally, provided it is done as soon as practicable.

Mandatory breach reporting will be a new process for Lions Clubs and Lions Charities. It is important that you understand, and have a plan in place, on how to respond to potential privacy breaches, otherwise you could face expensive fines as well as serious damage to your reputation.

If you need help with any privacy situation please let me know.

Alan Knowsley
MD202 Legal Counsel
legal@lionsclubs.org.nz