Key Things You Need to Know About NZ's Privacy Act

The Privacy Act 1993 is based around 12 principles which govern the collection, use, storage, access to and disclosure of personal data. Here is a summary of the key compliance points for the principles we are often asked to advise on.

Personal data must be collected from the individual concerned

- Wherever possible, collect data from the customer themselves.
- If you want to collect data about a customer from someone else (say as part of a credit check – but keep in mind there are other laws that apply to credit checks) then the customer must be informed and must consent.

Personal data must be collected for a legitimate purpose

- Only collect data that you really need for your business.
- Avoid the temptation to amass as much data as you can in case it might prove useful later. This concept of 'data minimisation' may yet be strengthened in New Zealand's Privacy Bill.

Personal data may only be used for the purposes for which it was collected

- Customers should be informed of all the purposes for which their data is being collected.
- For example, if you collect contact details for the purpose of a product sale, those contact details should not be used for other purposes such as marketing or promotional emails unless the customer was made aware of these additional purposes.

Only share personal data in limited circumstances

- Personal data must not be shared with others except in limited circumstances such as where the individual has consented to the disclosure, where the information was publicly available, or where disclosure was one of the purposes for which the information was collected.
- Be aware that this restriction applies to disclosure of personal data to your business's third-party service providers.

Be transparent

- In plain English: Tell customers about what information is being collected, what you are going to use it for, who you may share it with, whether the person has to give the information, and what will happen if they don't. This is where a clear and comprehensive privacy policy comes into play.

Keep personal data secure

- Ensure that personal data held by your business is protected through security, technical and other measures against loss and unauthorised access.
- Security breaches involving unauthorised access to, or the leaking of, personal data is perhaps one of the biggest reputational risks that businesses now face.

Don't hold personal data for longer than you are lawfully permitted

- Personal data can only be held for as long as is required for the purposes for which it was collected. For example, if you collect personal data from a person for the purposes of onboarding and maintaining them as a customer, if they cease to be a customer then that

personal data would generally no longer be required for the purpose for which it was collected.
- Personal data must also be disposed of securely.

Give people access to their personal data

- If a customer asks to see or correct their personal data, you must respond as soon as possible (and no later than 20 working days).

Ensure the accuracy of personal data

- Your business must take reasonable steps to ensure that personal data is accurate before using it.
- Also, if an individual makes a request to have their data corrected, you must respond to the individual informing them of the action taken as a result of the request. In most cases the appropriate action is likely to be correcting the data.

Key changes in the Pipeline by the Privacy Bill

At this stage it doesn't look like we will see substantial changes to these privacy principles when the Privacy Bill comes into force next year. However, there are still some important changes that are likely to occur – two of the more substantial being:

  - A mandatory obligation to report privacy breaches that are likely to cause serious harm; and
  - Restrictions on transferring personal data offshore. Broadly data will only be permitted to be transferred to an entity in another country if that country has privacy laws which are comparable to NZ or if there is a contract in place which provides the same level of protection.