NAVIGATING THE PRIVACY ACT 2020

Introduction: Reviewing Your Obligations

The regime around financial advice is changing and compliance is a regulatory requirement. The Privacy Act is being updated after 27 years (1993). This Act governs how individuals, organisations and businesses; collect, use, disclose, store and give access to personal information. In New Zealand, our approach is to apply these general principles called 'information privacy principles', derived from principles set out by a working group in the OECD in 1980. These principles were implemented to cover the life cycle of personal information through an agency. Agency is defined in the Act as '*a person or body of persons whether corporate or un-incorporate*'. Therefore, agencies must comply in relation to personal information which can identify an individual. Given the level of complexity, infinite variety and the enhancements within the technology space, the contextual nature of privacy has adapted. We are grappling with the question of how we deal with the implication of the new-fangled technology and the personal computer.

The concern on privacy has been increasing at a steady rate. The Privacy Commissioner has qualified these results through surveys completed every few years. In light of these concerns, the Law Commissioner has reviewed this Privacy Act and noted the following results; the fundamentals of the privacy act operate efficiently, however modernising is a crucial requirement. This Act has been completely rewritten to modernise the language and add the following seven key changes;

7 Key Changes:

1. *Mandatory privacy breach notification:* These implications are dependent on the level of breach and potential harm that could be caused. Notification must be provided to both the individual implicated and the Privacy Commissioner.

2. *Compliance notices:* The Privacy Commissioner can enforce and serve these notices to agencies. If Agencies don't comply or alter their processes, a fine of up to $10k can be charged.

3. *New criminal offences:* It is a criminal act to impersonate an individual to gain access or modify an individual's personal information.

4. *Binding decisions on access requests:* The Privacy Commissioner can now enforce these requests.

5. *Extraterritoriality:* If the Agency has business within New Zealand regardless of a physical presence, they are required to comply to this Act. Organisations often have arrangements with offshore business processing/outsource providers that can access the organisations systems and information to aid the service they provide (analytics). If there is no retainment of this information, the obligation remains with the agency.

6. *Strengthening cross-border protections:* The rules which govern sending information overseas.

7. *New refusal grounds:* A marginally increased ability for a Commissioner to enforce the Privacy Act.

Next steps for your business

This change in legislation provides an opportunity for all agencies to increase awareness, reiterate the respect of personal information and encourage staff to report any potential breaches. This could be accomplished by minimising the punishments that an agency may enforce on their employee's in question. The Privacy Commissioner maintains a variety of e-Learn training videos, freely accessible to facilitate knowledge. In addition, capturing lessons learnt is a great way to improve systems, reduce the risk of serious breaches and maintain a learning reference for staff.

It is important to prepare your agency and staff for the changes ahead. The Privacy Commissioner recommends agencies;

- Have an assigned Privacy Officer.
- Implement a privacy breach response plan to ensure personal information is used safely and stored securely.
- Update their privacy statements, including those enumerated on their websites, as websites are typically used as a central repository for easily accessible information. A free and accessible tool used to update your privacy statements is Pivomatic!, please refer to the Privacy Commissioner's website for access to templates.
- Ensure any overseas based service providers offer comparable privacy protections to New Zealand.

The thirteen principles within NZ's Privacy Act 2020 are listed below:

The Privacy Act Principles – 2020	
DATA COLLECTION	
1	**Only collect personal information you need** • Data minimisation principle. • Important to complete due diligence and legitimate regulatory needs. • Justify what you need and collect no more.
2	**Get it directly from the individual when possible** • The basis of this law is to restore and maintain individual autonomy. • The information we hold is on the trust of an individual.
3	**Be open about what you are going to do with it** • Majority of the complaints are caused by a lack of transparency and a consequence of surprise. Typically, when individuals aren't aware of the use of their information. • The legal obligation states that before collecting information, you should take reasonable steps to ensure that the individual is aware of the purposes.
4	**Be fair about how you get it** • Don't collect information by means that are unlawful, unfair or intrude to an unreasonable extent to the individual.
HOLDING PERSONAL INFORMATION	
5	**Keep it secure** • The law is prescriptive and although it does not state what these security standards are, it does ask companies to maintain a moving scale, dependent on the sensitivity of the information and the severity of the consequences if released.
6	**Let people see their own information** • An individual has the right to access and review what information has been stored about them. • As business often conduct staff vetting or hold personal information for employees, it is crucial employees only have access to review and update their own information. Company policy should incorporate a section to differentiate employee information verses client.
7	**Correct it if the person thinks it is wrong** • The individual is entitled to correct any errors they may notice captured in their personal information. If there is a dispute whether the information is accurate, a statement should be added noting this.
USE AND DISCLOSURE OF PERSONAL INFORMATION	

8	**Make sure it is accurate before you use it** • Take reasonable steps to ensure the information is correct, prior to acting on it.
9	**Dispose of it when you no longer need it** • You are required to hold on to client information for at least 7 years. • Remove or destroy irrelevant personal information securely. • Agency's policies and procedures should have a secure process in place.
10	**Only use it for the reason it was collected** • This has come under pressure as businesses are legally required to obtain information for purposes they never previously had (Covid tracing registers).
11	**Only share it if you have a good reason** • Personal information is only to be disclosed if directly related to the purpose of obtaining the information. For example, there is no obligation to notify the individual if the information is being shared with entities that are ancillary to providing that service. If an organisation routinely discloses information which is not an obvious part of consuming that service, there is an explicit obligation to notify the individual. • This could be disclosed to avoid a prejudice to the maintenance of the law, or when it is necessary to avoid a serious threat to an individual. Alternatively, to avoid prejudice to public health and safety.
12	**Only send it overseas if it will be adequately protected** • An organisation or business may only disclose personal information to an agency outside of NZ if the receiving agency is subject to similar safeguards to those within the Privacy Act. • If a jurisdiction does not offer similar protections, the individual concerned must be fully informed that their information may not be adequately protected, and they must expressly authorise the disclosure. • If you can't be satisfied, the obligation is to ensure the information is protected by other means, for example model contract clauses.
13	**Only use unique identifiers when it is clearly allowed** • Unique identifiers should only be used for the purpose for which it was obtained. Companies should not assign a unique identifier for your own customers that have been assigned to someone else.

If you have any questions, feel free to contact Compliance Refinery to discuss!

Reference: Financial Services Council NZ. (2020, October 5). *Get in Shape Session 10: Privacy - Reviewing your obligations under the Privacy Act* [Video]. YouTube. https://www.youtube.com/watch?v=Ns4UowQrD3k