VON MUENSTER LEGAL

PRIVACY

1. Introduction

Importance of Privacy Protection

In the wake of the ACCC's Digital Platforms inquiry, as well as various large-scale data and privacy breaches recently splashed across the news, ensuring privacy and data protection is more important now than ever before.

Advertising and Marketing agencies collect personal data and use it to target consumers during campaigns. It is important that such agencies are aware of their requirements under the *Privacy Act 1988* (Cth) (the **Act**) and the Australian Privacy Principles.

2. 13 Australian Privacy Principles:

1. **Open and transparent management of personal information** – this includes having an up to date Privacy Policy that is readily available
2. **Anonymity and pseudonymity** – should always give individuals an option to be anonymous or use a pseudonym
3. **Collection of solicited personal information** – can collect information the individual knows will be documented
4. **Dealing with unsolicited personal information** – Privacy Policy should set out clearly how the agency/organisation will deal with circumstances where unsolicited information is collected
5. **Notification of the collection of personal information** – individuals should always be aware when their information is being collected
6. **Use or disclosure of personal information** – individuals should always be made aware when and what personal information will be used or disclosed
7. **Direct marketing** – agencies or organisations may only use or disclose personal information freely given for direct marketing purposes
8. **Cross-border disclosure of personal information** – separate steps are required should this information be sent overseas
9. **Adoption, use or disclosure of government related identifiers** – there are limited circumstances where government data may be used, but only under very specific circumstances;
10. **Quality of personal information** – there should be reasonable steps taken to ensure that personal information is correct
11. **Security of personal information** – all reasonable steps should be taken to ensure that any personal information collected is kept safe
12. **Access to personal information** – individuals should be allowed to access the information held by agencies or organisations about them
13. **Correction of personal information** – agencies and organisations hold the responsibility to correct the information they have about individuals.

Who must comply?

If an agency or organisation is collecting, using or disclosing any 'personal information', the agency or organisation is required to comply with the Australia Privacy Principles.

What is 'Personal Information'?

The Australian Privacy Principles define 'Personal Information' as:

- Information or an opinion about an identified individual
- An individual who is reasonably identifiable.

The information about this individual that is considered personal may in given circumstances, include:

- Name, address, phone, email, photographs
- Social Data
- IP address, UDI, metadata, location, device information
- Use of cookies
- Any anonymous data that, read together, can be used to identify a person.

3. How can Agencies/organisations ensure they comply with the Australian Privacy Principles?

- Agencies and organisations should make it a top priority to ensure that they have an up to date and compliant Privacy Policy that is readily available and accessible
- Collection statement· should be particular to each circumstance where information will be collected (bespoke)
- Internal data collection handling practices should be developed.

4. Actions in relation to direct marketing

- Ensure that individuals have the capability of opting out SPAM emails and email communication marketing and advertising.
- An opt out notice needs to be clear and prominent in order to ensure individuals know they can opt out.
- There should be links to both the Agency/ organisations Privacy Policy and Collection

Statement.

5. Reportable data breach

The *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (**Amendment**) which came into force 22 February 2017 makes it mandatory for businesses to disclose certain data breaches.

The overriding purpose is to keep consumers safe from significant harm, and as such, heavy penalties of up to $1.8 million are in place in cases of non-compliance.

The Amendment applies to all businesses with responsibilities under the *Privacy Act 1988* (Cth). It provides that such organisations who have reasonable grounds to believe they have suffered an eligible data breach must notify affected individuals and the Office of the Australian Information Commissioner (**OAIC**). The Amendment also provides that an entity must give such notification if it has been directed to do so by the Commissioner.

The Amendment sets out a two-part test to determine what constitutes an eligible data breach:

1. There has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity, and

2. the access, disclosure or loss is likely to result in serious harm to any of the individuals *to whom the information relates.*

It is important to note that not all data breaches are made reportable under the Amendment. Only eligible data breaches, that is those likely to result in serious harm, are reportable. The difficult question is whether a breach is likely to result in serious harm.

6. ACCC Digital Platforms Inquiry

On 4 December 2017, the then-Treasurer, the Hon Scott Morrison MP, directed the ACCC to conduct an inquiry into digital platforms.

The inquiry looked at the effect that digital search engines, social media platforms and other digital content aggregation platforms have on competition in media and advertising services markets.

In particular, the inquiry looked at the impact of digital platforms on the supply of news and journalistic content and the implications of this for media content creators, advertisers and consumers. The final report was release on 26 July 2019.

The report sets out multiple ways that the Privacy Act could be amended to enhance protections for consumers, for example:

- Amending the definition of 'personal information' in the Act to include technical data, including all identifiers that could be used to distinguish individuals. This would bring breaches of data privacy into the remit of the Act and mean that consumers have the capability of benefitting from Privacy Act protections
- Requiring a better disclosure notice upfront for platforms collecting data explaining how a user's data will be collected, used and disclosed, with short terms and conditions written in plain language that is easy to understand
- An opt-in system for consumer to consent to the collection, use and disclosure of personal data. This would undoubtedly impact the amount of data that could be collected, used and disclosed as consumers become more aware of their rights to data privacy.

Other general recommendations of the inquiry are on the way, for example:

- A specialist digital platforms branch within the ACCC which will specialise in digital markets and use of algorithms;
- An inquiry (empowered by Ministerial direction) into tech services and advertising agencies; and
- Ongoing management of the Consumer Data Rights regime, including portability of data held by digital platforms e.g. banks.