RETAIL DRINKS AUSTRALIA

Retail Drinks Online Code - Privacy Guide

About this Privacy Guide

Under the *Privacy Act 1988* (the **Privacy Act**), Retailers (**Retailers** or **you**) are generally legally required to protect and manage 'personal information' in accordance with a set of detailed rules called the Australian Privacy Principles (or **APPs**) which form part of the Privacy Act.

The *Online Alcohol Sale and Delivery Code of Conduct* (**the Code**) has a number of principles which require Retailers to carefully consider how they deal with personal information to comply with their obligations under the Code. If you do not handle personal information in the correct way you may be in breach of the Privacy Act as well as your obligations under Code.

This Privacy Guide is designed to:

- help Retailers gain a basic understanding of key concepts under the Privacy Act and key requirements under the APPs; and
- give Retailers practical guidance regarding how to handle privacy issues when complying with the **Self-Exclusion** and **Third-Party Review Request** obligations under the Code.

This Privacy Guide is of a very general nature only and is not a substitute for legal advice. The examples provided are to illustrate key concepts. They are not an endorsement of the specific steps any individual Retailer should take.

Obligations under the Privacy Act are extensive and complex. Retailers will need to carefully consider their specific facts and circumstances which apply to them in order to comply with both the Privacy Act and the Code. These steps may be very different depending on the size and scale of the Retailer and other individual factors.

RETAIL DRINKS AUSTRALIA

UNDERSTANDING BASICS OF PRIVACY LAW

1. So what is 'personal information' and 'sensitive information'?

1.1 '**Personal information**' is basically any information, or an opinion, about an individual or an individual who is reasonably identifiable. This includes:

- obvious types of information which Retailers might collect, for example a Customer's name, telephone numbers, addresses (postal, email, etc), and age/date of birth in order to process an online order; and
- less obvious examples, particularly if they are combined with other data such as IP address of a computer or other devices or location data (e.g. from a mobile device's GPS). In some cases, the data collected from online 'cookies' and other online behavioural advertising technology may be classified as 'personal information' if you can reasonably identify a Customer from this data.

1.2 '**Sensitive information'** is a special subset of 'high grade' personal information, which includes health information, sexual orientation, religious beliefs, racial or ethnic origin, political association, criminal record and professional or trade association membership. For example, information relating to a Customer who is banned from purchasing alcohol due to any regulation imposed by a state or territory regulator is likely to be 'sensitive information'. Under the Privacy Act, very strict rules apply to this subset of personal information.

2. Why is privacy so important?

2.1 Failure to comply with the Privacy Act (such as serious and repeated breaches of the APPs) may give rise to substantial penalties or fines (currently up to $2.1 million for corporations). Breaches can also negatively impact reputation and could lead to expensive, time consuming and stressful legal proceedings or investigations.

2.2 Privacy issues, such a data breaches or the misuse of personal information are often 'front page news'. Privacy is now a key issues for Customers. According to the Office of the Australian Information Commissioner (**OAIC**) community attitude's survey: "Sixty-nine per cent of Australians say they are more concerned about their online privacy than they were five years ago".

RETAIL DRINKS AUSTRALIA

How to ensure privacy is protected - some general tips

While exceptions do apply, in general when you are handling or collecting personal information you should always:

- only collect the personal information which is strictly necessary for the purpose you are collecting it for (i.e., do not collect more personal information than you need);
- ensure that the personal information is necessary for one or more of your functions (for example, processing online orders, administrative functions or complying with obligations under the Code);
- only use or disclosure the personal information for the purpose for which it was collected; and
- consider how the personal information will be destroyed or de-identified once the purpose for which it has been collected has been completed (taking into consideration any legal record keeping requirements).

A high level summary of the APPs and some more general tips for compliance are set out in **Attachment A**.

RETAIL DRINKS AUSTRALIA

Privacy issues and key principles under the Code

This Section of the Privacy Guide provides Retailers with some practical guidance regarding how to handle privacy issues when complying with the **Self-Exclusion** and **Third-Party Review Request** obligations under the Code.

In addition to the key issues covered, Retailers should consider providing appropriate privacy training to staff regarding general privacy compliance as well as specific issues under the Code.

2.3 Self-Exclusion

Under Section 4.1.6 of the Code:

- *Online ordering systems must enable a Customer to self-exclude themselves from a delivery service for a specified period of time, or permanently.*
- *Self-exclusion must trigger a cessation of any direct or push marketing to the excluded Customer.*

This principle is known as **Self-Exclusion** under the Code.

2.4 Key privacy considerations and Self-Exclusion

Privacy issue	Practical tips to consider
Privacy Statement and Privacy Policy Under **APP 5** you are required to notify individuals of certain mandatory matters (including the purposes of collection) when you collect personal information from individuals (for example, if you collect personal information via an online Self-Exclusion form).	Retailers will need to: ▪ consider if they can integrate Self-Exclusion functionality into their online ordering systems. For example, this functionality may include an online form a Customer fills out to activate their Self-Exclusion. The Customer may be required to including details such as their name, contact details and Self-Exclusion preferences (e.g.,

This is often referred to as a 'privacy statement' or 'privacy collection notice'. This specific notification obligation is separate to having an **APP 1** Privacy Policy which generally describes how you handle personal information as an organisation.	specific period versus permanent). **A lower cost or simpler method** can simply be for a Retailer to advise customers to contact them if they wish to be excluded, and for the Retailer to then have an internal procedure to ensure this removes or suspends the customer's online account ▪ consider how to meet their APP 5 notification obligations. For example Retailers could include an APP 5 'privacy statement' or 'privacy collection notice' as part of the online form Customers populate to activate a Self-Exclusion ▪ consider if your organisation's Privacy Policy needs to be updated in light of the new Self Exclusion obligations
Use and disclosure of Personal Information Under **APP 6** you can only use and disclose personal information (such as the Customer's details) for the primary purpose for which it is collected (in this case to process a Self-Exclusion) and some limited secondary purposes (such as administrative functions). If a Retailer continues to use and disclose Personal Information of a Customer after Self Exclusion by that Customer, then the Retailer may potentially be in breach of APP 6.	Retailers will need to put in place systems and processes to ensure personal information collected for the purpose of Self-Exclusion is not used for any other purpose – such as direct marketing, discussed further below.

RETAIL DRINKS AUSTRALIA

Direct marketing Very strict rules also apply to direct marketing under **APP 7**, the Spam Act and telemarketing laws (**Direct Marketing Laws**). In some cases, under the Direct Marketing Laws direct marketing communications (such as e-News' letters, promotional SMS and snail mail Retailer catalogues) can only be sent if consent has been obtained. Separately, under the Code all and direct and push direct marketing communications must cease when a Customer Self Excludes If a Retailer continues to send direct or push marketing communications to a Customer after Self Exclusion, it will be in breach of the Code and may also be in breach of the Direct Marketing Laws.	Retailers will need to: ▪ have robust systems and processes in place for ensuring that Self-Exclusion requests are promptly acted upon. This includes ensuring that all direct or push marketing communications to the Customer have stopped **within five business days** from when the Customer activated the Self-Exclusion ▪ consider arrangements with any third party contractors – for example if a Retailer uses a third party marketing agency or platform to conduct direct or push marketing communications on its behalf to conduct marketing automation, such arrangements may need to be reviewed.
Destruction and deidentification of Personal Information Under APP 11 personal information is required to be securely stored and then deleted or de-identified when no longer required (subject to other legal obligations such as document retention laws). APP 11 is particularly relevant for when a Customer wishes to activate a permanent Self-Exclusion.	Retailers should consider: ▪ routinely reviewing their online and offline security arrangements to ensure personal information which it holds is adequately protected; ▪ when a Customer's records containing personal information should be deleted or de-identified if the Customer has activated a permanent Self-Exclusion (subject to other legal obligations such as document retention laws and reporting obligations under the Code); and

	▪ putting in place or updating relevant policies and procedures (such as a document retention policies) to account for permanent Self-Exclusion.

***Practical Example**: Jenny has decided to take part in 'Dry July'. She is regular Customer of Bobby Brings, an online alcohol delivery service which is a Retailer of Retail Drinks. Jenny logs into her online account for Bobby Brings where there is a section for Customer Self-Exclusion, she fills out the relevant online form and selects the option to Self-Exclude for a specified period (the Month of July only). Bobby Brings has included a privacy statement which explains all of the relevant APP 5 matters. The privacy statement also explains that by activating the Self-Exclusion for a specified period, Jenny will not receive direct or push marketing from Bobby Brings during that Self-Exclusion period. The Bobby Brings online system has been upgraded so that when a Self-Exclusion is activated, the online system reviews what marketing lists the Customer is on and automatically puts a hold on sending any direct or push marketing materials to the Customer. Jenny had previously signed up to receive Bobby Brings Monthly Newsletter and SMS promotions. She stops receiving these push and direct marketing communications for the month of July.*

2.5 Third Party Review Requests

Under Section 4.1.7 of the Code:

Retailers should provide the ability within their online ordering systems enabling a Third-Party to lodge a Request to review a Customer.

- *A Third-Party Request may relate to concerns as to whether ongoing supply to an online Customer complies with the Code, or state and territory laws. The Request may also relate to concerns regarding the Customer's alcohol consumption habits.*
- *Upon receipt of a Third-Party Request, and provided a Retailer does not form a view (acting reasonably) that the Third-Party Request is frivolous or being made for an improper purpose, a Retailer should conduct a review of the Customer with the potential (but not obligation) to raise the relevant concerns or risks with the Customer.*

- *Should the Retailer deem that further action is required, in addition to any other action the Retailer deems appropriate, the Customer who is the subject of action due to a Third-Party Request may be:*
  - *Advised that their ordering history has been reviewed; and*
  - *Provided relevant information and/or educational materials produced by government or third parties such as DrinkWise.*
  - *Due to privacy requirements, a Retailer can only confirm to the Third-Party lodging the original Request that the request was considered and reviewed, but cannot provide any further information and in particular, may not confirm what action (if any) was taken.*

Privacy issue	Practical tips to consider
Use and disclosure of Personal Information Under **APP 6** there are restrictions on the way an APP entity may deal with the personal information it holds, including whether and in what circumstances that information may be disclosed to a third party (including a relative such as a spouse). This means that if you disclose information about a Customer to a third party who has made a Third-Party Request you may be in breach of APP 6.	▪ Retailers will need to have robust systems and processes in place to ensure compliance with APP 6. Even revealing that an individual is a Customer of the Retailer may be a breach of APP 6 depending on the circumstance. ▪ In some cases, a party making a Third-Party Request may be persistent, angry or frustrated when you do not share personal information about a Customer. ▪ Consider how to respond to such requests such as: "*We can confirm that we have received your Third Party Request and we have taken appropriate steps in accordance with the Code. Due the privacy laws, we unfortunately can't give you any*

	personal information about a Customer or confirm if an individual is a Customer. But I can let you know that your Third-Party Request has been processed."
Under APP 5 you are required to notify individuals of certain mandatory matters when you collect Personal Information from individuals (for example, when a Customer first registers to be a Customer online).	▪ Retailers may wish to consider updating existing privacy collection statements to information Customers that their personal information may be used to review a Third-Party Request and that they may be contacted in relation to a Third Party Request. ▪ If you contact a Customer in respect of a Third-Party Request, you could consider informing the Customer of certain APP 5 matters at that point in time. Retailers could provide this information at the time they call or email a Customer in relation to the Third-Party Request.
APP 1 requires you to have an up-to-date privacy policy explaining how you generally collect, use and disclosure personal information	Retailers may wish to review their current privacy policy and update it to reflect that a Customer's personal information may be used in relation to a Third-Party Request, including to be contacted in relation to a Third Party Request.
There are very strict rules around the collection and use of 'sensitive information' (for example health records or criminal records). For example, under **APP 3** generally speaking such sensitive information can only be collected with consent of the individual.	Retailers should ensure as part of the Third-Party Request process, that they are not breaching any APP requirements in relation to sensitive information.

Destruction and deidentification of Personal Information

Under APP 11 personal information is required to be securely stored and then deleted or de-identified when no longer required (subject to other legal obligations such as document retention laws).

APP 11 is particularly relevant for when a Third-Party Review process has been conducted and closed.

Retailers should:

- routinely review their online and offline security arrangements to ensure Personal Information which it holds is adequately protected; and
- put in place or update policies and procedures (such as a document retention policy) to ensure that personal information is destroyed or deidentified when no longer required (subject to other legal obligation).

***Practical Example**: Brad is concerned about his wife Carolina's alcohol consumption. Carolina is a corporate executive who works a stressful job. Brad knows that Carolina regularly orders from Boutique Wines Online, a specialty wine online store. He goes onto Boutique Wines Online and lodges a Third-Party Request about Carolina. When Brad submits the Third-Party Request a "pop-up box" is displayed which states that the Third-Party Request has been successfully submitted and will be reviewed in accordance with the Code. The pop-up box explains that Boutique Wines Online cannot share any personal information about its Customers or confirm what action (if any) is taken in respect of a Third-Party Request. The Third-Party Request is reviewed by the Responsible Manager of Boutique Wines Online who determines that no further action is required under the Code. She does not contact Carolina. Brad emails Boutique Wines Online demanding to know what action has been taken and what his wife's ordering history is. The Responsible Manager of Boutique Wines Online contacts Brad and explains that all required steps have been taken under the Code. She explains that while she understands Brad's concerns, but due to strict privacy laws Boutique Wines Online can't share personal information about Customer's, including ordering history, even to a spouse. She directs Brad to the Retail Drinks website where he can see the Code for himself.*

RETAIL DRINKS AUSTRALIA

3. Where can I go to get more information about Privacy

- You can find more information about privacy and the protection of personal information on the website of the Office of the Australian Information Commissioner (**OAIC**) at www.oaic.gov.au
- The OAIC has published a number of useful guides which Retailers may find helpful including:
  - APP Guidelines
  - Guide to securing personal information
  - Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)

Attachment A - A General overview of the APPs

1. High Level Summary of the APPs

The below table sets out a very high level summary of the requirements under the APPs.

Topic	Relevant APPs	Summary
Consideration of personal information privacy	APP1 – APP2	An APP entity must adopt an open and transparent approach to their management of personal information including by implementing a privacy policy. Privacy should be a primary consideration at the commencement of any project and prior to implementation of new processes.
Collection of personal information	APP3 – APP5	An APP entity must collect personal information in accordance with the APPs including by providing individuals with specified mandatory information at the point of collection. Sensitive information must only be collected with consent, unless an exception applies.
Dealing with personal information	APP6 – APP9	There are restrictions on the way an APP entity may deal with the personal information it holds, including whether and in what circumstances that information may be used and disclosed (including offshore disclosure). There are specific requirements which apply in relation to use and disclosure of government related identifiers and use of personal information for direct marketing.
Integrity of personal information	APP10 – APP11	An APP entity must protect the personal information it holds from misuse, interference and loss and from unauthorised access, modification and disclosure. Personal information must be

		stored securely (whether it is in electronic or hard-copy format) and an APP entity must take reasonable steps to ensure it cannot be accessed by unauthorised persons, or tampered with. Once an APP entity no longer reasonably needs personal information which it holds for any permitted use or disclosure, it must destroy or de-identify the information (subject to any legal restrictions). The Privacy Act also contains a regime where serious data breaches (known as an eligible data breach) must be notified to the OAIC and individuals.
Access to, and correction of, personal information	APP12 – APP13	Individuals have the right to access and correct personal information which an APP entity holds about them. They also have the right to complain about an APP entity's compliance with the privacy laws. These rights only apply to the individual. You can't give information about a Customer to a third-party (see Section 2.5 of this Privacy Guide re Third-Party Requests).

2. Some practical general tips to comply with the APPs

- Manage personal information in an open and transparent way. This means privacy should be a key consideration whenever personal information is handled.
- Implement practices, procedures and systems to ensure compliance and adopt a privacy policy which meets the requirements of the APPs.
- Only collect personal information where reasonably necessary and do not collect more than you need 'just in case'. Where the personal information is also sensitive information consent is required.
- Collect personal information directly from the individual unless it is unreasonable or impracticable to do so. Individuals must be notified of certain mandatory information when their personal information is collected, usually through a collection statement.
- Only use or disclose personal information for the purpose it was collected, or a reasonably expected and related purpose. For sensitive information any secondary purpose must be directly related.
- Specific restrictions and accountability obligations apply to disclosure of personal information offshore including allowing somebody offshore to access it (even contractors or related bodies).
- Special rules apply in relation to 'government related identifiers' such as tax file numbers, Medicare and drivers licence numbers, and to the use of personal information for direct marketing purposes.
- Protect the quality and security of any personal information: ensure it is accurate and kept up-to-date and protect it from misuse, loss, unauthorised modification or disclosure. If you suspect a breach may have occurred seek legal advice as soon as possible.
- Do not keep personal information longer than is necessary for the purpose of collection or required by law.