

The New Australian Laws

The impact on marketing and
advertising in Australia

Australian Privacy Principles
Obligations Checklist

October 2013

ADMA Privacy Compliance Checklist

Background

Privacy issues are being reviewed globally. In most cases, technological changes are driving the demand for reforms and Australia is no exception. From 2004 – 2012 ADMA was involved in a review of the privacy laws which has led to the Privacy Amendment (Enhancing Privacy Protection) Act 2012. The new privacy legislation, including the changes affecting marketing will come into effect on 12 March 2014.

How to use this document

This **Australian Privacy Principles Obligations Checklist** document provides an organisation some key questions that need to be considered when updating their business practices to adhere to the updated privacy legislation that comes into effect on 12 March 2014. The checklist should be used as a guide when reviewing current practices and implementing new or updated practices.

Simply work your way through the checklist, comparing your current practices against the new legislation to identify if there are any areas where changes are required.

If you are uncertain about any of these legislation changes, please contact ADMA – comply@adma.com.au

APP 1 – open and transparent management of personal data		Check
General compliance with the APPs		
	<ul style="list-style-type: none"> Do you have a clear picture of your organisation's functions and activities? 	
	<ul style="list-style-type: none"> Have you completed a data audit that shows the movement of data, in, around and out of your organisation? 	
Your APP policy		
1.3	<ul style="list-style-type: none"> Do you have an APP privacy policy? 	
	<ul style="list-style-type: none"> Does your privacy policy discuss the functions and activities of your organisation? 	
	<ul style="list-style-type: none"> Does your privacy policy discuss the way in which you collect, hold, use and disclose personal data? 	
	<ul style="list-style-type: none"> Is your privacy policy kept up to date? 	

1.4	<p>Does your privacy policy include the following information?</p> <ul style="list-style-type: none"> • The kind of personal data that you collect and hold, • How you collect and hold personal data, • The purpose for which you collect, hold, use and disclose the data, • How an individual may request to see a copy of the personal data held by you, • How an individual may seek the correction of their personal data, • How an individual may make a complaint to you for not complying with the APPs, • How you will deal with any complaint, • Whether you will or whether you are likely to disclose personal data to a party that is overseas (this includes your own related parties and any third party that you may outsource any functions or activities), and • If you are likely to disclose personal data to an overseas recipient, then have you listed the countries in which these recipients are located. 	
Availability of your APP policy		
1.5	Is your privacy policy readily available?	
	Is your privacy policy available in more than one form (by soft copy and by hard copy)?	
	Is your privacy policy available for free?	
1.2	<p>Have you taken reasonable steps to implement practices, procedures and systems relating to your entities functions and activities that will help ensure?</p> <ul style="list-style-type: none"> • That you comply with the APPs, and • Will enable you to deal with enquiries or complaints in relation to your compliance with the APPs. 	

APP 2 – Anonymity and pseudonymity		Check
2.1	<ul style="list-style-type: none"> Do you provide your consumers the option of engaging with you without using their name or even their real name? 	
	<ul style="list-style-type: none"> Is it necessary for you to collect personal data in order to deliver a service to a consumer? 	
	<ul style="list-style-type: none"> Can you still service the individual if they don't provide you with a name or even their real name? Note - If it is impractical to engage with the individual without their personal data, then you do not have to provide them with the option of being anonymous or the option to use a pseudonym. 	

APP 3 – Collection of solicited personal data		Check
Collecting personal information		
3.1	<ul style="list-style-type: none"> Do you collect personal data? 	
	<ul style="list-style-type: none"> Do you collect personal data that is directly related to, one or more of your functions or activities? 	
Collecting sensitive data		
3.3	<ul style="list-style-type: none"> Do you collect sensitive data? 	
	<ul style="list-style-type: none"> Do you make sure that you have the express consent of the individual before you collect sensitive data? 	
	<ul style="list-style-type: none"> Do you ensure that the sensitive data that you collect is reasonably necessary for one or more of your organisations functions or activities? 	
Collecting data from third parties		
3.6	<ul style="list-style-type: none"> Do you collect personal data from third parties? For example, social media, mobile apps or third party lead generation or list providers 	
	<ul style="list-style-type: none"> Before collecting data from third parties, have you considered whether it is unreasonable or impracticable to obtain the personal data directly from the individual? 	

APP 4 – Dealing with unsolicited personal data		Check
4.1	<ul style="list-style-type: none"> Have you received any personal data that you have not specifically requested from an individual? 	
4.3	<ul style="list-style-type: none"> If you have received any personal data from an individual that you did not request, do you have procedures in place to either destroy or de-identify the data? Note – if the data you have received is something you could have directly obtained from the individual, then you do not have to delete or de-identify the data. 	

APP 5 – Notification of collection of personal data		Check
5.1	<ul style="list-style-type: none"> Do you have a notification statement? 	
	<ul style="list-style-type: none"> Have you customised your notification statement so that it can be used within your website, e-mail, social media and in writing? 	
	<ul style="list-style-type: none"> Is your notification statement, sent to or delivered to, an individual, at or before or as soon as practicable after you collect personal data from an individual? 	
5.2	<p>Does your notification statement include the following?</p> <ul style="list-style-type: none"> Your identify and contact details The fact that you may collect personal data from a third party source If you collect personal data from a third party source, the type of data that you collect and the circumstances of that collection If you collect personal data from a third party, the names of those parties or a description of the types of those parties The purpose of the collection Whether any collection of personal data is required or authorised by law The consequences to the individual if all or some of their personal data is not collected by you Any other party or type of party that you may disclose the personal data that you collected That your APP privacy policy contains data about how an individual can access and seek correction to their personal data that is held by you That your APP privacy policy includes data about how an individual can complain about a breach of the APPs, and how you will deal with such complaints received Whether you are likely to disclose personal data to an overseas recipient If you are likely to disclose personal data to an overseas recipient, then have you also listed the countries or the likely countries of the overseas recipients 	

APP 6 – Use or disclosure of personal data		Check
Primary Purpose Rule		
6.1	<ul style="list-style-type: none"> • Do you check to ensure that you use or disclose personal data for the primary purpose for which it was collected? 	
Secondary Purpose Rule		
6.2	<p>Option 1</p> <ul style="list-style-type: none"> • Do you disclose personal data for any secondary purpose? <ul style="list-style-type: none"> ○ If so, do you check to see if you hold the individual's consent for the use and disclosure their personal data for the secondary purpose? 	
	<p>Option 2</p> <ul style="list-style-type: none"> • Do you disclose personal data for any secondary purpose? <ul style="list-style-type: none"> ○ If so, have you considered if the individual would reasonably expect you disclose the data for a secondary purpose? and, ○ Is the secondary purpose related to the primary purpose? 	
Related bodies corporate		
6.6	<ul style="list-style-type: none"> • Do you collect personal data from a related body corporate? <ul style="list-style-type: none"> ○ Note - Where a related body corporate has collected the data for a purpose and you then collect the data from the related body corporate then the same purpose is applied to you when you receive the data from the related body corporate. This means, you cannot apply another purpose to the data. • Do you check to ensure that you comply with the primary purpose rule? (above) OR <ul style="list-style-type: none"> ○ Do you check to ensure that you comply with the secondary purpose rule (above)? 	

APP 7 – Direct Marketing	Check
7.2	<p>Option 1</p> <p>Have you collected personal data from the individual?</p> <ul style="list-style-type: none"> • Would the individual <u>reasonably expect</u> you to use or disclose their personal data for marketing purposes? AND • Have you provided the individual with a simple and easy means by which they can opt-out from receiving marketing communications? AND • Have you checked to ensure that the individual has not opted out of receiving marketing communications? <p>If you answered yes to all of these, then you may use the personal data for marketing purposes.</p>
7.3	<p>Option 2</p> <p>Have you collected personal data from an individual?</p> <ul style="list-style-type: none"> • Would the individual <u>not reasonably expect</u> you to use or disclose their personal data for marketing purposes? AND • Has the individual consented to the use or disclosure of their personal data for marketing purposes? OR <ul style="list-style-type: none"> ○ Is it impracticable to obtain the individual’s consent? AND • Have you provided the individual with a simple and easy means by which they can opt-out from receiving marketing communications? • Have you ensured that the opt-out is included within each marketing communication to the individual OR <ul style="list-style-type: none"> ○ Have you included a statement within the marketing communication that makes the individual aware that they can make an opt out request? • Have you checked to ensure that the individual has not opted out of receiving marketing communications? <p>If you answered yes to all of these, then you may use the personal data for marketing purposes.</p>

7.3	<p>Option 3</p> <p>Have you collected personal data from a third party?</p> <ul style="list-style-type: none"> • Has the individual consented to the use or disclosure of their personal data for marketing purposes? OR <ul style="list-style-type: none"> ◦ Is it impracticable to obtain the individual's consent? AND • Have you provided the individual with a simple and easy means by which they can opt-out from receiving marketing communications? • Have you ensured that the opt-out is included within each marketing communication to the individual? OR <ul style="list-style-type: none"> ◦ Have you included a statement within the marketing communication that makes the individual aware that they can make an opt out request? • Have you checked to ensure that the individual has not opted out of receiving marketing communications? <p>If you answered yes to all of these, then you may use the personal data for marketing purposes.</p>	
7.4	<ul style="list-style-type: none"> • Do you use an individual's sensitive data for marketing purposes? • Have you obtained the consent of the individual before using their sensitive data for marketing purposes? 	
7.6	<p>Do you use or disclose personal data to facilitate direct marketing by third parties?</p> <p>If so, do you ensure the individual may:</p> <ul style="list-style-type: none"> • Request not to receive any marketing communications from you AND • Requests that you not use or disclose their personal data to third parties AND • Request that you provide the source of that information 	
7.7	<ul style="list-style-type: none"> • When an individual requests not to receive direct marketing communications from you; <ul style="list-style-type: none"> ◦ Do you ensure that you do not apply a fee? ◦ Do you comply with the individual's request within a reasonable period? 	

	<ul style="list-style-type: none"> • When an individual requests that you not use or disclose their personal data to other organisations for marketing purposes; <ul style="list-style-type: none"> ○ Do you ensure that you do not apply a fee? ○ Do you comply with the individual's request within a reasonable period? 	
	<ul style="list-style-type: none"> • Where an individual requests that you provide the source from which you obtained their personal information, do you notify them within a reasonable period of time? 	

APP 8 – Cross border disclosure of personal data		Check
8.1	<ul style="list-style-type: none"> • Do you disclose personal data that you collected to any party that is located overseas? • Before doing so, do you take reasonable steps to ensure that the overseas recipient will not breach the APPs? 	
8.2	<ul style="list-style-type: none"> • You do not need to take reasonable steps to ensure the overseas entity does not breach the APPs if you can satisfy either of the following: <ul style="list-style-type: none"> ○ You reasonably believe the overseas recipient is subject to similar laws as the APPs in order to protect the individuals personal data; <i>AND</i> ○ There are mechanisms that an individual can use to enforce the protection of the overseas laws. 	
	<ul style="list-style-type: none"> • Have you informed the individual that you will be disclosing their personal data to an overseas party? • If so, has the individual then consented to the disclosure of their personal data to an overseas party? 	

APP 9 – Adoption, use or disclosure of government identifiers		Check
9.2	<ul style="list-style-type: none"> • Do you collect any government related identifiers from individuals? • If so, you may only use or disclose the government identifiers in order to verify the identity of the individual for the purposes of your organisations functions or activities. 	

APP 10 – Quality of personal data		Check
10.1	<ul style="list-style-type: none"> Do you take reasonable steps to ensure that the personal data that you collect is accurate, up-to-date and complete? 	
10.2	<ul style="list-style-type: none"> Do you ensure that any use or disclosure of personal data, having regard to the purpose, is accurate, up-to-date, complete and relevant? 	

APP 11 – Security of personal data		Check
11.1	<ul style="list-style-type: none"> Do you take reasonable steps to protect the personal data that you collect? Do you take reasonable steps to ensure the personal data that you collect is protected from misuse, interference and loss? Do you take reasonable steps to ensure the personal data that you collect are protected from unauthorised access, modification or disclosure? 	
11.2	<ul style="list-style-type: none"> Do you take reasonable steps to ensure that you destroy or de-identify personal data when you no longer require that data? 	

APP 12 – Access to personal data		Check
12.1	<ul style="list-style-type: none"> Upon request, are you able to readily provide an individual with access to their personal data? 	
12.8	<ul style="list-style-type: none"> Do you apply a fee for any request by an individual? <p>Note – any such fee must not apply to the making of the request.</p>	
12.9	<ul style="list-style-type: none"> Have you declined an individual access to their personal data? If so, have you given the individual a written notice setting out the following; <ul style="list-style-type: none"> The reason for the refusal, Why it would be unreasonable to grant the access <i>AND</i> The means by which the individual may complain about the refusal. 	

APP 13 – correction of personal data		Check
13.1	<ul style="list-style-type: none"> • Do you ensure that the personal data that you hold is accurate, up-to-date, complete, relevant and not misleading? • Do you receive any requests to correct the personal data that you hold by the individual? • Have you made the correction within a reasonable time? 	
13.2	<ul style="list-style-type: none"> • Have you notified any other APP Entity of the corrections that you have made to the personal data? <ul style="list-style-type: none"> ○ You must do so because of a correction you have made or at the request of the individual. ○ However, you do not need to make this notification if it is impracticable to do so? 	
13.3	<ul style="list-style-type: none"> • Have you elected to decline a request to correct the personal data? <p>If so, have you given the individual a written notice setting out the following;</p> <ul style="list-style-type: none"> ○ The reason for the refusal, ○ Why it would be unreasonable to make the correction <i>AND</i> ○ The means by which the individual may complain about the refusal. 	
13.5	<ul style="list-style-type: none"> • Have you made the correction within a reasonable time? 	

Privacy & Marketing Compliance Short Course



The purpose of this course is to cover the main regulations which a marketing executive would encounter on a regular basis. The course addresses a number of key areas:

- Advertising content
- Impact of Privacy Law changes
- Data collection, management and use
- Other Australian legislation: Spam Act, Do-not-call, Do-not-mail, Social media and mobile.

Find out more and register:

<http://www.adma.com.au/learn/short-courses/privacy-and-marketing-compliance/>