

PRIVACY POLICY CHECKLIST

This checklist is intended for use when formulating your organisation's privacy policy. Seek legal advice to verify that the final policy complies with your organisation's legal and regulatory environment.

ACTION

Introduction

- Consider the nature and language style of the policy that will suit your clients/customers
- Consider whether a brief overview should be included in the introduction, or whether a summary should be included
- Identify the name of your organisation and any related organisations covered by the policy
- Consider if any additional general information about the organisation and its operations is required
- Explain that personal information will be handled by those organisations in accordance with the privacy policy and the Australian Privacy Principles' (APP's) and any applicable laws, regulations, codes etc.
- Specify the types of personal information covered by the policy
- Identify the person in your organisation who is responsible for the policy
- Include a statement of commitment to privacy compliance
- Indicate whether or not the policy is a publicly accessible document
- If appropriate, refer to any other relevant policies, procedures, documents

Collection

- Explain:
 - what types of personal information are collected
 - what "personal information" covers
 - any other key terms used in the policy
 - in general terms, how personal information is collected
 - the purposes for which the information is collected
 - if there is a legal requirement to provide any of the information
 - the main consequences of not providing the information.
- Specify that the organisation only collects personal information:
 - that is reasonably necessary for, or directly related to, one or more of the organisation's functions
 - lawfully and fairly and not in an unreasonably intrusive way.

Use

- Specify generally how the organisation uses the personal information it collects
- If some uses are likely to be considered more privacy intrusive, be more specific about how the information is used

Disclosure

Specify generally the circumstances in which personal information could be disclosed.

Identify the recipients or classes of recipients, for example:

- for delivery of products/services that the client/customer has requested
- for provision of any outsourced services
- to law enforcement authorities investigating suspected unlawful conduct.

Marketing

Explain how personal information could be used by the organisation for direct marketing and marketing analysis purposes

Specify what options individuals have to opt out of (or opt in) receiving direct marketing materials.

If applicable, explain circumstances in which personal information might be disclosed to third parties for marketing purposes

If applicable, explain that the organisation may from time to time facilitate product offerings from third parties but in doing so does not disclose personal information to those entities

If personal information is licensed to third parties, be explicit about the circumstances

Explain if marketing analysis is undertaken only using de-personalised and/or aggregated data

Data quality

Explain the steps taken to keep personal information accurate, complete and up-to-date

New products and services

Describe the steps taken to assess and address any privacy impacts of new technologies that might be adopted or new products and services that might be introduced

Security

Explain that the organisation takes reasonable steps to protect personal information it holds from:

- misuse and loss
- unauthorised access, modification or disclosure.

Indicate that when personal information is no longer required, reasonable steps are taken to destroy or permanently de-identify the information

Access

Explain that individuals may obtain access to their own personal information

Specify the name and/or title of the person who is the contact for requests for access

Set out when access might not be granted

If applicable, indicate that the organisation might charge for providing access to personal information but that such charge would not be excessive and would not apply to making the request

If any personal information is considered by an individual to be not accurate, complete and up-to-date, invite the individual to request correction of the information

Government identifiers

Explain that, although at times the organisation might request details regarding certain government assigned identification numbers, the organisation:

- only does so where it is necessary and lawful
- does not use such identifiers as its own.

Trans-border data flows

Explain the circumstances in which personal information might be transferred outside Australia

Sensitive information

Explain the circumstances in which sensitive information might be collected

Explain the types of sensitive information that might be collected

Contact details and complaints

Specify how individuals can contact a representative of the organisation in relation to privacy of personal information and correction of incorrect information

Specify the way in which complaints may be lodged and how those complaints will be handled

Other

Give general information about:

- review and monitoring processes.
- any privacy review program.

Consider:

- if it is appropriate to include employee privacy principles and procedures in the policy
- if there should be references to other relevant documents.

Miscellaneous:

- insert the date and version number of your organisation's policy
- specify your organisation's procedures to vary the privacy policy
- identify who is responsible for the privacy policy within the organisation
- include any copyright notices or trademarks.

CPA AUSTRALIA COPYRIGHT NOTICE

Copyright © CPA Australia Ltd ("CPA Australia") (ABN 64 008 392 452), 2012. All rights reserved. All trade marks and trade names are proprietary to CPA Australia and must not be downloaded, reproduced or otherwise used without the express consent of CPA Australia. You may access and display these materials on your computer, monitor or other video display device and make one printed copy of any whole page or pages for your personal use only. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act 1968 (Cth) (or any other applicable legislation throughout the world), or as otherwise provided for herein, you may not use these materials in any manner without the prior written permission of the copyright owner.

DISCLAIMER

CPA Australia and the author have used reasonable care and skill in compiling the content of these materials. However, CPA Australia makes no warranty as to the accuracy or completeness of any information contained therein nor does CPA Australia accept responsibility for any acts or omissions in reliance upon these materials. These materials are intended to be a guide only and no part is intended to be advice, whether legal or professional. All persons are advised to seek professional advice to keep abreast of any legal or other reforms and developments. To the extent permitted by applicable law, CPA Australia, its employees, agents and consultants exclude all liability for any loss or damage claims and expenses including but not limited to legal costs, indirect special or consequential loss or damage (including but not limited to, negligence) arising out of the information in the materials. Where any law prohibits the exclusion of such liability, CPA Australia limits its liability to the resupply of the information.