**PRIVACY POLICY SELF-ASSESSMENT TOOL**

**INFORMATION PRIVACY PRINCPLE 5**

PRIVACY POLICY SELF-ASSESSMENT TOOL

Information Privacy Principle (**IPP**) 5 requires an organisation to have a document that clearly sets out its policies on the management of personal information, and to make it available to anyone that asks for it. This document is commonly referred to as a privacy policy.

This self-assessment tool is designed to assist organisations developing and/or reviewing their privacy policy.

PRIVACY POLICY LOCATION AND ACCESSIBILITY

This section focuses on how the policy can be found online and how accessible it is. While the only requirement under the *Privacy and Data Protection Act 2014* (**PDP Act**) is that your organisation have a privacy policy, OVIC recommends that the guidance offered be considered by your organisation to reflect openness and transparency.

|  |  |  |
| --- | --- | --- |
| Question | Response | Comment |
| Does your organisation have a privacy policy?  IPP 5 requires that every organisation covered by the PDP Act has a public facing privacy policy. |  |  |

|  |  |  |
| --- | --- | --- |
| Findability of privacy policy | Response | Comment |
| **Is** **the policy available on your organisation’s website?**  OVIC recommends that organisations make their privacy policy available online. |  |  |

|  |  |  |
| --- | --- | --- |
| Content | Response | Comment |
| **How can the policy be found on your organisation’s website?**  Consider providing users with multiple ways to find the policy. Does your organisation’s website have a separate privacy statement (that is, a statement which generally covers how information is automatically collected from a user because of a visit to a website), in which a link to the privacy policy is made available, or can it be found by searching ‘privacy’ in the search bar. Alternatively, is it practicable for your organisation to create a dedicated privacy webpage which explains the need to know information about privacy, and how to contact your organisation about a privacy concern, as well as providing a copy of the detailed policy. |  |  |
| **Are there other policies that affect privacy?**  Consider referring to other policies that affect privacy (or better provide a link to it) such as CCTV Policy, Complaints Handling Policy or Health Records Policy, as the user may be interested in them. |  |  |
| **Are there any other documents or information that complement the policy?**  Consider whether your organisation should develop additional information such as a FAQ fact sheet, or simplified fact sheet about information privacy, that compliments the privacy policy. Also consider linked related policies and information about your organisation’s Freedom of Information process. |  |  |

|  |  |  |
| --- | --- | --- |
| Accessibility of privacy policy | Response | Comment |
| **Is the policy available as a webpage?** |  |  |
| **Is the policy available as a downloadable PDF?**  Victorian Government digital standards suggests that PDF should not be relied upon, as the format is hard to make compliant with the Web Content Accessibility Guidelines (WCAG) 2.0. The standards suggest that a PDF document be made into a HTML alternative, and that content of a PDF should appear as an accessible webpage also. |  |  |
| **The policy available as a downloadable Word document?**  Victorian Government digital standards suggests that downloadable documents such as a Microsoft Word document, should not be relied upon, as the format is hard to make compliant with the WCAG. The standards suggest that a document be made into a HTML alternative, and that content of the document should appear as an accessible webpage also. |  |  |
| **Is the policy available in other languages?**  This is not a requirement however, consider whether there is a need to make the policy, or any information about privacy, available in other languages. |  |  |
| **Is there an audio version of the policy?**  This is not a requirement. |  |  |
| **Can the policy be shared?**  For example, can it be shared onto social media or to email? This is not a requirement. |  |  |
| **Is there more than one version of the policy on the website?**  Ensure that any drafts or outdated policies are removed from your organisation’s website, as they may cause confusion for users searching for your current policy. |  |  |

POLICY CONTROL

This section focuses on the administrative details of the organisation’s policy.

All the guidance made is a minimum requirement. An organisation may have its own requirements on what information is to be included in the policy.

|  |  |  |
| --- | --- | --- |
| Question | Response | Comment |
| Does the policy identify the organisation? |  |  |
| Does the policy state what version it is?  OVIC recommends, at a minimum, that a policy should contain a version number. |  |  |
| Does the policy have a date?  OVIC recommends, at a minimum, that a policy should contain a date. |  |  |
| Does the policy have a review date?  OVIC recommends, as best practice, that a policy have a clear statement when the policy is due for a review. |  |  |

POLICY CONTENT

This section focuses on the content of the policy; both what is covered and how it is written and presented. Organisations are encouraged to think about privacy broadly, not just in the legal sense, and a policy should not be a mirror of the legislation.

Consider whether it is appropriate to present the discussion of the IPPs in themes, or to tell a narrative of how information flows through your organisation. For example, from how and why it is collected, to how it is used and stored, to when it is destroyed or transferred.

|  |  |  |
| --- | --- | --- |
| Layout | Response | Comment |
| Is the policy broken up into sections with clearly marked headings? |  |  |
| Is the policy layered?  For example, providing a brief summary of your organisation’s privacy policy on a webpage, form, sign or poster, and then referring or providing a link to the full privacy policy. |  |  |
| Content | Response | **Comment** |
| Does the policy reference current privacy legislation? |  |  |
| Does the policy state the organisation’s main functions? |  |  |
| Does the policy state the types of personal information it generally collects, and for what purpose?  IPP 1 - Collection  This includes a statement as to whether collection of personal information is compulsory or optional. |  |  |
| Does the policy state how the organisation uses and discloses the personal information?  IPP 2 - Use and disclosure  This includes a statement as to the types of third parties the information may be shared with. |  |  |
| Does the policy state how the organisation ensures the personal information it collects is accurate, complete and up to date?  IPP 3 - Data quality |  |  |
| Does the policy state how the organisation stores and manages personal information, including how long personal information may be stored for?  IPP 4 - Data security  OVIC recommends that at a minimum, reference should be made to the *Public Records Act 1973* and any other relevant legislation or schedule.  Also consider whether your organisation is subject to the Victorian Protective Data Security Framework (VPDSF) and accompanying obligations under Part 4 of the PDP Act. |  |  |
| Does the policy contain information about how an individual can request to access and/or alter their personal information?  IPP 6 - Access and correction  OVIC recommends that, as a default position, organisations adopt the processes in the *Freedom of Information Act 1982* (if subject to the FOI Act) for allowing individuals to access and correct their personal information. |  |  |
| Does the policy state whether the organisation assigns unique identifiers to individuals, and if so, under what circumstances?  IPP 7 - Unique identifiers |  |  |
| Does the policy state that a person may remain anonymous when dealing with the organisation?  IPP 8 - Anonymity |  |  |
| Does the policy state how privacy is protected if information is transferred or stored outside of Victoria?  IPP 9 - Transborder data flows  This IPP also applies to personal information that is stored on cloud computing services, which can be stored outside of Victoria. |  |  |
| Does the policy state whether the organisation collects sensitive information?  IPP 10 - Sensitive information |  |  |
| Does the policy include information about any other relevant legislation (State or Federal)?  Consider whether your organisation needs to mention the *Health Records Act 2001* (Vic) and the *Health Privacy Principles,* the *Privacy Act 1988* (Cth) and the Australian Privacy Principles, or the General Data Protection Regulation (GDRP), or any other relevant privacy legislation.  If your organisation has separate policies that affect information privacy, OVIC recommends it is mentioned or a link is provided in the privacy policy. |  |  |
| Complaints | Response | **Comment** |
| Does the policy explain how to make a privacy complaint to your organisation? |  |  |
| Does the policy include current details on how to contact your organisation?  For example email, phone number, postal address or online complaint form. |  |  |
| Is there a separate policy for general complaint handling?  If there is a separate complaint handling policy, OVIC suggests that it is linked or mentioned in the privacy policy. |  |  |
| Does the policy correctly direct complaints to OVIC? |  |  |
| Does the policy include a description of OVIC’s functions?  For example, OVIC’s role is to try and resolve privacy complaints through a conciliation process. |  |  |
| Does the policy include current OVIC details?  For example, links to OVIC website, email, phone number, postal address. |  |  |
| If relevant, does the policy correctly direct complaints to other external complaints bodies such as the Health Complaints Commissioner or Office of the Australian Information Commissioner?  Ensure correct contact details are provided for any additional complaints bodies. |  |  |

**Disclaimer:** The information in this document is general in nature and does not constitute legal advice.