

**Appendix 7—Privacy of personal information**

**Part I: Contractual clauses to ensure privacy of personal information**

<b>ASSURANCE MAP OUTCOME</b>	<b>Green: Very low level of assurance required</b>	<b>Light Blue: Low level of assurance required</b>	<b>Medium Blue: Medium level of assurance required</b>	<b>Dark Blue: High level of assurance required</b>
<b>Green: Very low level of assurance required</b>	<p><b>Contractual clause:</b></p> <p>The <b>Provider:</b></p> <ul style="list-style-type: none"> <li>• Undertakes to comply with the Privacy Act 2020 (see Part II below).</li> <li>• The undersigned undertakes to comply with the Health Information Privacy Code and other relevant codes relating to the handling of personal information.</li> <li>• Acknowledges that the <b>Purchasing Agency</b> has the right to audit provider when requested.</li> </ul>			
<b>Light Blue: Low level of assurance required</b>	Same as first column, plus:	<p><b>During the contracting process the provider will be required to sign a form confirming they:</b></p> <ul style="list-style-type: none"> <li>• Understand and will conform to the requirements of the Privacy Act, Health Information Privacy Code and other relevant codes.</li> <li>• Understand the significance of personal information and have appropriate controls in place to manage personal information.</li> <li>• Will report all privacy incidents to the Ministry’s Privacy Officer within 24 hours of the incident occurring.</li> </ul>		
<b>Medium Blue: Medium level of assurance required</b>	Same as the first and second columns, plus:		<p><b>During the contracting process the provider will be required to:</b></p> <ul style="list-style-type: none"> <li>• Provide the Ministry with a copy of their privacy policy, which includes breach/incident definitions and a Privacy Officer, for the Ministry</li> </ul>	

ASSURANCE MAP OUTCOME	Green: Very low level of assurance required	Light Blue: Low level of assurance required	Medium Blue: Medium level of assurance required	Dark Blue: High level of assurance required
			<p>Privacy Officer to review. If they do not have one, they will be required to describe their plans to develop one and any mitigating controls currently in place.</p> <ul style="list-style-type: none"> <li>• Provide evidence that privacy is adequately included in their assurance plan (for example, internal audit reports).</li> </ul> <p><b>Contractual clause:</b></p> <ul style="list-style-type: none"> <li>• When requested, the <b>Provider</b> will complete a privacy survey.</li> <li>• The <b>Provider</b> may not sub-contract without getting permission from the Ministry first.</li> <li>• The <b>Provider</b> will report all privacy incidents to the Ministry's Privacy Officer within 24 hours of the incident occurring.</li> </ul>	
<p><b>Dark Blue:</b></p> <p>High level of assurance required</p>	<p>First column not applicable</p>	<p>Same as the second and third columns above, plus:</p>		<p><b>During the contracting process the provider will be required to:</b></p> <ul style="list-style-type: none"> <li>• Provide an up-to-date privacy framework which includes a staff training programme and a breach reporting process. The Ministry has the right to audit and request random spot checks regarding privacy management.</li> </ul> <p><b>Contractual clause:</b></p> <ul style="list-style-type: none"> <li>• The <b>Purchasing Agency</b> has the right to audit and request random spot checks regarding privacy management:</li> <li>• The <b>Purchasing Agency</b> has the right to review the <b>Provider's</b></li> </ul>

<b>ASSURANCE MAP OUTCOME</b>	<b>Green: Very low level of assurance required</b>	<b>Light Blue: Low level of assurance required</b>	<b>Medium Blue: Medium level of assurance required</b>	<b>Dark Blue: High level of assurance required</b>
				privacy framework following a privacy incident. <ul style="list-style-type: none"> <li>• The <b>Purchasing Agency</b> has the right to hold mandatory privacy meetings/ workshops between the <b>Purchasing Agency</b> and the <b>Provider</b> once a quarter or following a privacy incident.</li> <li>• The <b>Provider</b> undertakes to make periodic assurance reports on the effectiveness of the privacy framework.</li> </ul>

**Part II: Contractual clauses to ensure compliance with the Privacy Act 2020**

The undersigned provider undertakes to observe the requirements of the Privacy Act 2020 and the information privacy principles by putting the following measures in place:

1. Ensure that the project will not require more personal information than necessary: only the amount of information specifically required will be collected.
2. Ensure that the collection of personal information is:
  - a. Authorised—The business owner takes responsibility for the collection, and is accountable for it.
  - b. Lawful—The project has good bases in law and policy.
- c. Reasonable—Information is not collected in an intrusive manner.
3. Communicate to individuals the purpose of collecting information—A privacy statement informs individuals the reason for their information being collected by the project.
4. Ensure that effective controls are in place to protect against the loss, misuse, or disclosure of personal information.
5. Ensure that individuals are able—
  - a. To obtain copies of their own personal information collected by the project; and
  - b. To ask for corrections of any errors in that information.
6. Ensure that the project will maintain the accuracy of personal information and keep it up to date.
7. Ensure that the personal information collected is not kept for longer than necessary.
8. Ensure that the personal information will not be used for purposes other than that for which it was collected.