



Privacy Compliance Assessment Survey

A. Is the organization accountable for its information practices?

1. Has the organization designated an individual (or individuals) to be responsible for its compliance with the *Personal Information Protection Act* (PIPA)?
 Yes No
2. Has the organization developed and implemented the necessary policies and practices to meet its obligations for the proper handling of personal information?
 Yes No
3. Does the organization use contracts and/or other means to ensure that contractors providing services on its behalf that involve the collection, use or processing of personal information provide privacy protection equal to or superior to its own?
 Yes No
4. Has the organization developed and implemented a complaint process to handle complaints about its personal information practices?
 Yes No

B. Does the organization identify purposes?

5. Does the organization identify the purpose(s) for which personal information is needed and how it will be used, taking into account both primary and secondary purposes (i.e. audit, marketing, subscription renewals etc.)?
 Yes No
6. Does the organization inform the individual, either verbally or in writing, of the purposes for collecting the personal information before or at the time that it collects personal information?
 Yes No
7. Before using personal information for a new purpose, not previously identified, does the organization inform the individual of the new purpose and obtain consent prior to its use?
 Yes No

C. Does the organization obtain consent?

8. Does the organization obtain consent from the individual whose personal information is collected, used or disclosed?
- Yes No
9. Does the organization, when obtaining consent, inform the individual of the purposes for the collection, use or disclosure of personal information in a manner that is clear and can be reasonably understood?
- Yes No
10. Does the organization obtain the individual's consent before or at the time of collection, as well as when a new use is identified?
- Yes No
11. Does the organization obtain consent **without** using deceptive means or false or misleading information about how personal information will be used?
- Yes No
12. Does the organization **not** make consent a condition for supplying a product or a service unless the collection, use or disclosure of the personal information is necessary to provide the product or service?
- Yes No
13. Does the organization, in determining what form of consent to use (e.g. written, verbal, deemed, or opt-out), consider both the sensitivity of the personal information and what a reasonable person would expect and consider appropriate in the circumstances?
- Yes No
14. Does the organization permit an individual to withdraw consent to the collection, use or disclosure of personal information unless it would frustrate the performance of a legal obligation?
- Yes No
15. Does the organization, upon receipt of a notice to withdraw consent, inform the individual of the likely consequences of withdrawing consent, when the consequences are not obvious?
- Yes No

D. Does the organization limit its collection of personal information?

16. Does the organization only collect personal information for purposes that a reasonable person would consider appropriate in the circumstances?

Yes

No

17. Does the organization limit the amount and type of personal information it collects to only that which is reasonable to fulfill the purpose(s)?

Yes

No

18. Does the organization collect personal information directly from the individual it is about unless the Act authorizes the collection of personal information from another source?

Yes

No

E. Does the organization limit its use, disclosure and retention of personal information?

19. Does the organization use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances?

Yes

No

20. Does the organization use or disclose personal information only for the purpose(s) for which it collected it, unless the individual consents to a new purpose, or the use or disclosure is otherwise authorized by the Act?

Yes

No

21. Does the organization retain personal information only as long as is reasonable for legal or business purposes?

Yes

No

22. Does the organization either anonymize the information or destroy the records containing personal information once the information is no longer needed?

Yes

No

F. Does the organization ensure that personal information is accurate and complete?

23. Does the organization make reasonable efforts to ensure that the personal information it collects, uses or discloses about an individual is accurate and complete?

Yes

No

G. Does the organization secure personal information?

24. Does the organization make reasonable security arrangements (including physical measures, technical tools, and organizational controls where appropriate) to protect personal information in its custody or under its control?

Yes No

25. Does the organization, in determining what level of security arrangements are reasonable, take into account the sensitivity of the personal information in its custody or under its control?

Yes No

26. Does the organization implement safeguards that protect personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal by individuals both outside the organization as well as within?

Yes No

27. Does the organization have in place security measures that protect personal information regardless of the format in which it is held (e.g. paper, electronic, audio, video)?

Yes No

28. Does the organization dispose of or destroy personal information in a way that prevents unauthorized parties from gaining access to it?

Yes No

29. Does the organization have a process in place for notifying the Office of the Information and Privacy Commissioner if an incident occurs that involves loss of or unauthorized access to or disclosure of personal information that may pose a real risk of significant harm to individuals?

Yes No

H. Is the organization open about its information practices?

30. Does the organization make the following information available to customers, clients and employees on request?

(a) brochures or other information that explain its personal information policies and practices?

Yes No

(b) name or position name or title and contact information of the person who is accountable for its personal information policies and practices?

Yes No

(c) name or position name or title and contact information of the person who can answer questions about its purposes for collecting personal information?

Yes No

(d) how an individual can gain access to his or her personal information and the name or position name or title and contact information of the person to whom access requests should be sent?

Yes No

(e) the process for making a complaint about its personal information practices (e.g. the process for making internal complaints as well as complaints to the Information and Privacy Commissioner)?

Yes No

I. Does the organization allow individuals access to their personal information and a right to request corrections?

For Access to Personal Information Requests

31. Does the organization, upon request, provide applicants with:

(a) access to their personal information, subject to limited exceptions?

Yes No

(b) an explanation of how their personal information is or has been used?

Yes No

(c) a list of any individuals or organizations to which their personal information has been disclosed?

Yes No

32. Does the organization provide a copy of the information requested or a response that includes reasons for not providing access:

(a) within 45 calendar days unless an extension of time is permitted under the Act?

Yes No

(b) for a reasonable cost?

Yes No

33. Does the organization, if all or part of the requested personal information is refused, provide the applicant with a response that includes:

(a) reasons and the provision(s) of the Act on which the refusal is based?

Yes No

(b) the name and contact information of someone who can answer the applicant's questions about the refusal?

Yes No

(c) information on how to request a review by the Information and Privacy Commissioner?

Yes No

For Correction of Personal Information Requests

34. Does the organization, upon request, correct personal information that is found to be inaccurate or incomplete?

Yes

No

35. Does the organization, if a correction is made, send a copy of the corrected personal information to each organization to which the incorrect or incomplete information was disclosed, if reasonable to do so?

Yes

No

36. Does the organization, if no correction is made in response to an individual's request, annotate the personal information in dispute (i.e. make a note) to indicate that a correction was requested but not made?

Yes

No

J. Does the organization have a process for handling complaints?

37. Does the organization have a process in place for receiving and responding to complaints or inquiries about its personal information practices?

Yes

No

38. Does the organization investigate all complaints?

Yes

No

39. Does the organization, where a complaint is justified, take appropriate measures to rectify the situation including correcting information handling practices and policies where necessary?

Yes

No

For more information

Additional information and resources about PIPA are available on the websites of Access and Privacy, Service Alberta, and the Office of the Information and Privacy Commissioner.

Access and Privacy Service Alberta

Phone: 780-644-PIPA (7472) Toll free dial 310-0000

E-mail: pspinfo@gov.ab.ca

Website: pipa.alberta.ca

Office of the Information and Privacy Commissioner

Phone: 403-297-2728 Toll free dial 1-888-878-4044

E-mail: generalinfo@oipc.ab.ca

Website: www.oipc.ab.ca

Acknowledgements: This document was developed by Corporate Privacy and Information Access, Ministry of Management Services, Government of British Columbia. It has been adapted and reproduced by the Access and Privacy, Service Alberta. We would like to thank our colleagues in British Columbia for allowing us to adapt this information for use in Alberta.