
The Privacy Audit

In order for an organization to identify what it needs to do to comply with the *Personal Information Protection Act* (PIPA), it is necessary to determine the current state of its personal information holdings and related procedures. The organization needs to know what it has in the way of personal information, where it is stored and how it is currently managed.

A privacy audit involves the following three steps, which may be performed together or in order: taking an inventory of your personal information holdings; identifying the information needs of the different functions within your organization; and identifying your current information practices. This would include how and why your organization collects, uses and discloses personal information.

A privacy audit should be an internal function. It is a self-assessment tool. There is no obligation to make the findings public. Therefore, it is important to stress to staff participating in this audit that it is not a test. Its purpose is not to embarrass them or to call people to task. What is needed at this stage in the development of the privacy program is an accurate and thorough inventory and analysis. There are no right answers. The sole purpose of the audit should be to collect information that can inform the planning and decision-making process regarding the future application of privacy legislation to the organization.

Taking an Inventory

Begin the audit by taking an inventory of the organization's existing records and information management policies and practices. The time and effort involved in this process will vary depending upon the complexity of the personal information holdings.

For example, the organization may collect personal information about the public, customers, partners, employees, contractors, shareholders, vendors, and many other types of individuals. For each function in the organization, you will need to determine if it collects, uses or discloses any personal information and, if so, how that information is managed and by whom.

When identifying the organization's personal information holdings, be sure to examine records in hardcopy, on computers and other electronic media, as well as any online resources (e.g. websites, chat rooms, news services, mailing lists, or bulletin boards) it operates.

While not an exhaustive list, the following areas commonly collect, use and disclose personal information:

- customer service
- complaints
- human resources
- finance/purchasing
- information technology
- security
- legal services

Additionally, you should think of all the points where the organization collects personal information. Examples may include:

- point-of-purchase
- customer service numbers
- kiosks
- contests
- e-mail
- surveys
- video cameras
- audio tapes
- marketing lists
- loyalty programs
- delivery services
- warranties
- bankruptcies
- returns
- application forms
- order forms
- websites
- bulletin boards
- chat rooms
- call centre
- technology enablers

The main benefit of this inventory is to enable you to determine the extent to which PIPA will apply to the organization's functions and the necessary scope of the privacy program you will need to develop. For example, if the organization only has personal information about its employees, the scope of the privacy program will be much more limited than an organization that also has personal information relating to customers or other types of individuals with whom it does business.

Follow Up the Inventory by Identifying Information Needs and Practices

Once you have determined what personal information the organization has and where it is held, the next step is to fully understand how and why the personal information is collected, used and disclosed. A necessary follow-up to the inventory is to identify the information needs of the different functions within the organization, along with current information practices.

To do this, you will need to determine how and why all the types of personal information the organization has are necessary to a particular function and to the organization's operation. The reasons why personal information is collected, used and disclosed, along with who can see what, when, where, how and why, all need to be identified, documented and analyzed. This is an essential step if you want to know if the information management practices comply with the Act.

In order to audit the organization's information needs and practices, you could use questionnaires, in-depth interviews, group discussions, file and policy reviews, sampling, or other means of identifying information practices. Regardless of the methods, the review should be comprehensive and cover all of the organization's operations.

Audit questions could include:

1. How does the organization collect personal information? Common ways in which organizations collect personal information include standard forms, customer surveys, loyalty programs, online interaction, video cameras.
2. Why does the organization collect the personal information? Does the organization need it for a function or activity?
3. Are individuals likely to be aware that the organization is collecting their personal information?

4. Does the organization inform individuals of the purpose for collecting their personal information?
5. Does the organization obtain consent from individuals before collecting or using their personal information? If so, what processes (verbal statements, paper or electronic notices) are used to obtain consent?
6. How does the organization use personal information? (e.g. for specific business functions, for activities that solicit new business.)
7. Does the organization disclose personal information to anyone outside the organization?
8. Does the organization make individuals aware of the intended uses and disclosures of their personal information? If so, how are individuals informed?
9. Is the personal information the organization holds accurate and complete to the extent necessary for the purpose of the collection, use or disclosure?
10. How does the organization store personal information? (e.g. paper files, cabinets, databases, audio, video)?
11. Where does the organization store personal information? (Organizations may keep personal information stored in a single cabinet or database or it may be spread across the organization in a number of sites.)
12. Who has access to the personal information held by the organization and who actually needs to have that access?
13. Does the organization have measures to protect the personal information it holds from unauthorized access, collection, use, disclosure, copying or modification from individuals both within and outside the organization?
14. Does the organization contract out any functions or activities involving personal information? Does the organization take any privacy measures to protect this information?
15. Is personal information collected, processed or stored by a service provider outside of Canada on behalf of the organization?
16. How long does the organization retain personal information?
17. How does the organization destroy or dispose of personal information?
18. If a privacy breach occurs, does the organization have processes in place to determine whether notification to the Information and Privacy Commissioner is required, and to mitigate possible harm to individuals as a result of the breach?

Once this information is obtained, it should be analyzed to determine whether the organization's information-handling practices comply with PIPA.

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 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.