II.A.3 Conduct a Privacy Audit

A privacy audit will help your private sector organization determine what personal information you're currently collecting, where it is stored and how it is managed. This is a crucial step in assessing what you must do to comply with the ten principles of privacy protection.

How to Conduct an Audit

A privacy audit is a straight forward process that requires two steps:

1. Take an inventory of your personal information holdings
2. Identify the information needs and practices of the different areas within your organization

A privacy audit is an internal process and there is no obligation to make the findings public. It is important to stress to employees participating in the audit that it isn't an evaluation or test. The privacy audit is a thorough inventory and analysis designed to inform the planning and decision-making process.

The amount of time and resources you need to devote to a privacy audit will depend on the size of your organization, the amount of personal information you hold, and the complexity of your information handling practices.

Take an Inventory

Begin the audit by taking an inventory of your organization's existing records and information management policies and practices. Completing this inventory will help you determine the scope of the privacy policy you need to develop.

First, determine which areas collect, use or disclose personal information and how it's managed. For reference, the following business areas commonly collect, use and disclose personal information:

- Customer service
- Complaints
- Human resources
- Finance/purchasing
- Information technology
- Security
- Legal services

Second, determine all of the points of contact within your organization involving personal information, such as:

- Customer service telephone numbers
- Points-of-purchase
- Kiosks
- Contests
- E-mail
- Surveys
- Video cameras

- Audio tapes
- Marketing lists
- Loyalty programs
- Delivery services
- Warranties
- Bankruptcies
- Returns
- Application forms
- Order forms
- Web sites
- Bulletin boards
- Chat rooms
- Call centres

When identifying the organization's personal information holdings, be sure to examine records stored in hardcopy, on internal computers, in other electronic media and in online resources.

Identify Information Needs & Practices

Once you have determined what personal information your organization has and where it is held, the next step is to fully understand why and how it's used. You must document and analyze the personal information needs and information management practices of each area within your organization. Your goal is to determine:

- If the personal information being collected, used or disclosed is actually necessary to a particular function or operation
- Who can see what, when, where, how and why

To gather this information, you can use questionnaires, in-depth interviews, group discussions, file and policy reviews, sampling or other means. Audit questions could include:

- How does the organization collect personal information? (standard forms, customer surveys, loyalty programs, online interaction, videos etc.)
- Why does the organization collect the personal information? Does the organization need it for a function or activity?
- Are individuals made aware that the organization is collecting their personal information?
- Does the organization inform individuals of the purpose for collecting their personal information?
- Does the organization obtain consent from individuals before collecting or using their personal information? If so, what processes are used to obtain consent? (verbal statements, paper or electronic notices etc.)

- How does the organization use personal information? (for specific business functions, for activities that solicit new business etc.)
- Does the organization disclose personal information to anyone outside the organization?
- Does the organization make individuals aware of the intended uses and disclosures of their personal information? If so, how are individuals informed?
- Is the personal information the organization holds accurate, complete and up-to-date?
- How does the organization store personal information? (paper files, databases, audio files, video files etc.)
- Where does the organization store personal information? (single cabinets, databases, sites spread across the organization etc.)
- Who has access to the personal information held by the organization and who actually needs to have that access?
- 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?
- Does the organization contract out any functions or activities involving personal information? Does the organization take any privacy measures to protect this information?
- How long does the organization retain personal information?
- How does the organization destroy or dispose of personal information?

Regardless of the method used, the privacy audit must be comprehensive and cover all of your organization's operations.

Information & Privacy Commissioner

The Office of the Information and Privacy Commissioner offers a number of tools and resources for private organizations.

Legislation

- *Personal Information Protection Act*

Contact Information

Office: 250 356-1851

Email: privacy.helpline@gov.bc.ca