

New Privacy Legislation, What You Should Know

Privacy Questionnaire (from the Privacy Commissioner's Web site)

The following are some common sense questions you can use to help your organization implement the Personal Information Protection and Electronic Documents Act. The questionnaire may be used along with the description of the Act in this guide.

If you are unsure about whether or when the Act applies to your organization, please refer to the section *Is your organization subject to the Act* of this guide.

Not all of the following questions will apply to all organizations, as the Act applies to a wide variety and size of organizations. Consider each question along with your organization's current practices. Answering "no" indicates areas that need to be addressed or improved.

Personal information holdings

- Do you know what personal information is?
- Do you collect, use or disclose personal information in your day-to-day commercial activities?
- Do you have an inventory of your personal information holdings?
- Do you know where personal information is held (physical locations and files)?
- Do you know in what format(s) the personal information is kept electronic, paper, etc.)?
- Do you know who has access to personal information in and outside your organization?

Accountability of organization and staff

- Have you named a privacy officer who is responsible for your organization's overall compliance with the Act?
- Is this responsibility shared with more than one person?
- If these responsibilities are shared, have they been clearly identified?
- Can your staff respond to internal and external privacy questions on behalf of the organization, or do they know who should respond?
- Does your staff know who receives and responds to:
 - requests for personal information?
 - requests for correction?
 - complaints from the public?
- Do your customers know whom to contact:
 - for general inquiries regarding their personal information?
 - to request their personal information?
 - to request corrections to their personal information?
 - for complaints?
- Is your privacy officer able to explain to the public the steps and procedures for requesting personal information and filing complaints?
- Has your staff been trained on the Act?

Will there be ongoing training?

- Is your staff able to explain the purposes for the collection, use and disclosure of personal information to customers in easy to understand terms?
- Is your staff able to explain to customers when and how they may withdraw consent and what the consequences, if any, there are of such a withdrawal?
- Will you inform your employees of new privacy issues raised by technological changes, internal reviews, public complaints and decisions of the courts?

Information for customers and employees

- Do you have documents that explain your personal information practices and procedures to your customers?
- Does this information include how to:
 - obtain personal information?
 - correct personal information?
 - make an inquiry or complaint?
- Does this information describe personal information that is:
 - held by the organization and how it is used?
 - disclosed to subsidiaries and other third parties?
- Do you have a privacy policy for your web site?
- Is your privacy policy prominent and easy to find? Is it easily understandable?
- Do your application forms, questionnaires, survey forms, pamphlets and brochures clearly state the purposes for the collection, use or disclosure of personal information?
- Have you reviewed all your public information material to ensure that any sections concerning personal information are clear and understandable?
- Have you ensured that the public can obtain this information easily and without cost?
- Is this information reviewed regularly to ensure that it is accurate, complete and up to date?
- Does this information include the current name or title of the person who is responsible for overseeing compliance with the Act?

Limiting collection, use, disclosure and retention to identified purposes

- Have you identified the purposes for collecting personal information?
- Are these purposes identified at or before the time the information is collected?
- Do you collect only the personal information needed for identified purposes?
- Do you document the purposes for which personal information is collected?
- If you gather and combine personal information from more than one source, do you ensure that the original purposes have not changed?
- Have you developed a timetable for retaining and disposing of personal information?
- When you no longer require personal information for the identified purposes or it is no longer required by law, do you destroy, erase or make it anonymous?

Consent

- Does your staff know that an individual's consent must be obtained before or at the time they collect personal information?
- Does your staff know they must obtain an individual's consent before any new use or new disclosure of the information?
- Do you use express consent whenever possible, and in all cases where the information is sensitive or the individual would reasonably expect it?
- Is your consent statement worded clearly, so that an individual can understand the purpose of the collection, use or disclosure?
- Do you make it clear to customers that they need not provide personal information that is not essential to the purpose of the collection, use or disclosure?

Third party transfers

- Do you use contracts to ensure the protection of personal information transferred to a third party for processing?
- Does the contract limit the third party's use of information to purposes necessary to fulfil the contract?
- Does the contract require the third party to refer any requests for access or complaints about the information transferred to you?
- Does the contract specify how and when a third party is to dispose of or return any personal information it receives?

Ensuring accuracy

- Is personal information sufficiently accurate, complete and up to date to minimize the possibility that your organization might use inappropriate information?
- Does your organization document when and how personal information is updated, to ensure its accuracy?
- Do you ensure that personal information received from a third party is accurate and complete?

Safeguards

- Have you reviewed your physical, technological and organizational security measures?
- Do they prevent improper access, modification, collection, use, disclosure and/or disposal of personal information?
- Is personal information protected by security safeguards that are appropriate to the:
 - sensitivity of the information?
 - scale of distribution?
 - format of the information?
 - method of storage?
- Have you developed a "need-to-know" test to limit access to personal information to what is necessary to perform assigned functions?

- Has your staff been trained about security practices to protect personal information? For example, is staff aware that personal information should not be left displayed on their computer screens or desktops in their absence?
- Is your staff aware that they should properly identify individuals and establish their right to access the personal information before disclosing it?
- Do you have rules about who is permitted to add, change or delete personal information?
- Is there a records management system that assigns user accounts, access rights and security authorizations?
- Do you ensure that no unauthorized parties may dispose of, obtain access to, modify or destroy personal information?

Requests for access to personal information

- Is your staff aware of the time limits the law allows to respond to access requests?
- Can you retrieve personal information to respond to individual access requests with a minimal disruption to operations?
- Do your information systems facilitate the retrieval and accurate reporting of an individual's personal information, including disclosures to third party organizations?
- Do you provide personal information to the individual at minimal or no cost?
- Do you advise requesters of costs, if any, before personal information is retrieved?
- Do you record an individual's response to being notified of the cost of retrieving personal information?
- Do you provide personal information in a form that is generally understandable? (For example, do you explain abbreviations?)
- Does your organization have procedures for responding to requests for personal information in an alternate format (such as Braille or audio tapes)?

Handling complaints

- Can an individual easily find out how to file a complaint with you?
- Do you deal with complaints in a timely fashion?
- Do you investigate all complaints received?
- Are your customer assistance and other front -line staff able to distinguish a complaint under the law from a general inquiry? If unsure, do they discuss this with the individual?
- Do you advise individuals about all available avenues of complaints, including the Privacy Commissioner of Canada?
- Are staff responses to public inquiries, requests and complaints reviewed to ensure they re handled fairly, accurately and quickly?
- When a complaint is found to be justified, do you take appropriate corrective measures, such as amending your policies and advising staff of the outcome?