

FURTHER INFORMATION

Quebec is the only province that currently has legislation deemed substantially similar to the federal law. Organizations in Quebec are subject to that province's legislation and are, therefore, exempt from the federal act for *intra-provincial matters only*.

CONTACT:

Commission d'accès
à l'information
Du Québec

QUÉBEC CITY
575 rue Sainte-Amable
Bureau 1.10
Québec (Québec) G1R 2G4
Telephone: (418) 528-7741
Toll Free: 1-888-528-7741
Fax: (418) 529-3102
Web site: www.cai.gouv.qc.ca
Email: cai.communications@cai.gouv.qc.ca

FEDERAL INFORMATION:

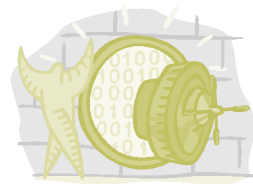
The Office of the Privacy Commissioner of Canada
112 Kent Street,
Ottawa, ON K1A 1H3
Telephone: (613) 995-8210
Toll free: 1-800-282-1376
Fax: (613) 947-6850
Web site: www.privcom.gc.ca
Email: info@privcom.gc.ca

A.T.U. CANADIAN COUNCIL

1450 Meyerside Drive, Suite 701,
Mississauga Ontario,
L2N 2T5

TEL: (905) 670-4710 FAX: (905) 670-3659

Email: atucouncil@bellnet.ca



5. LIMIT USE, DISCLOSURE AND RETENTION

- Unless new consent was given or the use or disclosure is authorized by the Act, use or disclose personal information only for the purpose for which it was originally collected.
- Keep personal information only as long as necessary to satisfy the purposes and put procedures in place for retaining and destroying that information

6. BE ACCURATE

- Minimize the possibility of using incorrect information by applying the following checklist for accuracy:
 - List specific items of personal information required to provide a service.
 - List the location where all related personal information can be retrieved.
 - Record the date when the personal information was obtained or updated.
 - Record the steps taken to verify accuracy, completeness and timeliness of the information. This may require reviewing the records or communicating directly with the individual concerned.

7. USE APPROPRIATE SAFE-GUARDS

- Protect personal information against loss, theft, unauthorized access, disclosure, copying, use or modification.
- Use appropriate safeguards in the form of physical measures (locked filing cabinets, restricted access to offices, alarm systems); technological tools (passwords, encryption, firewalls); organization controls (limiting access on a 'need to know' basis, clauses and letters of agreement, staff training).
- Make sure personal information that has no relevance to the transaction is either removed or blocked out when providing copies of information to others.

8. BE OPEN

- Ensure that your executive members are familiar with the procedures for responding to individual inquiries regarding his or her personal information.
- Provide a description of what personal information is made available to other organizations and why it is disclosed.
- Information about these practices should be made available to all members.

9. GIVE INDIVIDUALS ACCESS

- If requested, inform individuals if you have any personal information about them and give them access to it.
- Explain how it is or has been used and provide a list of any organizations to which it has been disclosed.
- Correct or amend any personal information if its accuracy is challenged.
- Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in Section 9 of the Act .

10. PROVIDE RECOURSE

- Inform complainants of the avenues of recourse. The A.T.U.'s procedure is to attempt to resolve it at the local level first, through the National Office second, and, lastly, via the Office of the Privacy Commissioner.
- Take appropriate measures to correct information handling practices and policies.
- Investigate ALL complaints received:
 - Record the date a complaint is received and the nature of the complaint (e.g. delays in responding to a request, incomplete/inaccurate responses, improper collection, disclosure, use or retention).
 - Acknowledge receipt of the complaint immediately.
 - Assign the matter to a person with the skills necessary to review it in a fair and impartial manner. Provide them with access to the relevant records and those who initially handled the request for that information.
 - Correct any inaccurate personal information and/or modify policies and procedures based on the outcome of a complaint.

THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)



A GUIDE FOR
CANADIAN
A.T.U.
LOCALS

DEFINITIONS

Personal Information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- Age, name, ID numbers, income, ethnic origin, or blood type;
- Opinions, evaluations, comments, social status, or disciplinary actions;
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (e.g. to change jobs)

Personal information does not include the name, title or business address or telephone number of an employee or organization.

Commercial activity includes any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, **membership** or other fund-raising lists.

Organization includes as association, a partnership, a person or a **trade union**.

Consent implies a voluntary agreement with what is being done or proposed. Consent can either be express or implied. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Disclosure means making personal information available to others outside of the organization.

Use refers to the treatment and handling of personal information within an organization.

WHAT IS NOT COVERED BY THE ACT?

The collection, use or disclosure of personal information by federal government organizations listed under the *Privacy Act*.

Provincial or territorial governments and their agents.

An employee's name, title, business address or telephone number.

An individual's collection, use or disclosure of personal information strictly for personal purposes (e.g. personal greeting card list).

An organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes.

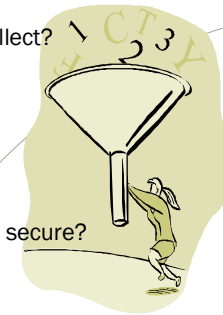
Employee information-except in the federally-regulated sector.



TOP TEN PRINCIPLES

1. BE ACCOUNTABLE

- **Protect all personal information held by your local or transferred to a third party for processing.**
- **Appoint an individual to be responsible for your local's compliance and communicate this to your membership.**
- **Analyze all personal information handling practices using the following checklist:**
 - What personal info do we collect?
 - Why do we collect it?
 - How do we collect it?
 - What do we use it for?
 - Where do we store it and is it secure?
 - Who has access?
 - When and how is it disposed of?
- **Obtain consent before disseminating any member's personal information!**
- **Ensure information is correct, complete and current.**
- **Include a privacy protection clause in contracts to guarantee that the third party provides the same level of protection as the A.T.U. does.**
- **Limit use of the personal information to the purposes specified to fulfill the contract.**
- **Limit disclosure of the information to what is authored by the A.T.U. or required by law.**
- **Consent clauses should be easy to find, use clear concise language, do not use blanket categories for use, be specific as possible about which organizations handle the information.**



2. IDENTIFY THE PURPOSE

- **Clearly outline your purposes for collecting data so individuals can understand how the information will be used or disclosed.**
- **Examples of purposes can include, but are not limited to, providing benefits to employees, sending out union membership information, opening an account, establishing eligibility for special offers or discounts.**

- **Record all identified purposes and obtained consents for easy reference in case an individual questions the use of such information.**

3. OBTAIN INFORMED CONSENT

- **Inform the individual, in person, by phone, by mail, by fax, via email, etc., in a clear concise manner of the purposes for the collection, use or disclosure of the data.**
- **Obtain consent before or at the time of collection and identify if it is being used differently than on previous occasions when consent was granted.**
- **Inform the individual of how the information will be used and explain the ramifications of the refusal or withdrawal of their consent.**
- **The form of consent should take into consideration:**
 - Reasonable expectations of the individual
 - Circumstances surrounding the collection.
 - Sensitivity of the information involved.
- **Never obtain consent by deceptive means.**
- **Do not make consent a condition for supplying a product or service unless the requested information is required to fulfill an explicitly specified and legitimate purpose.**

4. LIMIT COLLECTION

- **Do not collect personal information indiscriminately but only gather it for what is needed for the identified purposes.**
- **Collecting less information lowers the cost of storing and archiving data and also reduces the risk of inappropriate uses and disclosures.**
- **Identify the type of personal information that you collect in your information-handling policies and practices and ensure that members are cognizant of why the information is required.**

Continued on reverse

