

WHAT DO CANADA'S NEW PERSONAL INFORMATION LAWS REQUIRE?

Equifax is pleased to provide its members with this second bulletin in a series prepared by BLG describing highlights of the Personal Information Protection and Electronic Documents Act (Canada) ("Bill C-6") and similar provincial laws. These bulletins are not intended as legal advice on any particular facts; we urge you to consult your legal advisor as to any specific issues related to the needs of your organization in complying with these laws.

1. What is your basic obligation? Bill C-6 requires you, in your collection, use and disclosure of **"personal information"** in the course of **"commercial activities"**, to comply with the ten principles of the Model Code for the Protection of Personal Information which is Schedule 1 to the Act. An organization that operates a "federal work, undertaking or business" must do the same with personal information about its employees.

2. **What is "personal information"?** Information about an "identifiable individual"; it does not include the name, title, business address or business phone number of an employee of an organization, but it is not clear just where the lines will be drawn. In particular, it is not limited to information provided by the individual concerned or by someone on his or her behalf: in Québec, the commission which administers privacy laws has ruled that internal memos on an insurance company's claim file were personal information which the claimant was entitled to see.

There is an exception for information that is "publicly available", as specified by regulations under the Act. The regulations refer to: (1) names, addresses and telephone numbers in the phone book (if the subscriber has the option of being unlisted); (2) magazines, books, newspapers, or other publications available to the public, where the individual has provided the information; (3) publicly available databases or registries; (4) court records; and (5) business or professional directories. Personal information from (3), (4) or (5) can be used without consent only to the extent that its collection, use and disclosure relate directly to the purpose for which the information appears in the database, registry, record or directory.

Until January 1, 2002, Part 1 will not apply to "personal health information".

3. **What is a "commercial activity"?** A particular transaction, act or conduct (or regular course of conduct) "of a commercial character"; it specifically includes selling, bartering or leasing donor, membership or other fundraising lists. It is not clear how broadly this will be interpreted.

4. **Identify your purposes** Before you collect personal information, identify the purposes for which you are collecting it, and in particular what you are going to use it for, and to whom outside the organization you are going to disclose it.

5. **GET CONSENT!** This is the single most important principle in Part 1. The individual must consent to the collection, use and disclosure of personal information relating to him or her. This does not necessarily mean the individual must sign a formal written consent: the kind of consent required depends on the sensitivity of the information and the reasonable expectations of the individual. In some cases, consent may be implied; in others, it may take the form of a "negative option" (i.e., "check this box if you do not want us to give your information to other fundraisers"); in others, an "express yes" may be needed, orally or in writing.

Once given, consent may be withdrawn.

There are a number of exceptions to the consent requirement. Some are specific to the collection or use of information; some are specific to disclosure. Other than the "publicly available" exception referred to above, most of these are of a "legal", "medical" or "governmental" nature, and will not be much use to business organizations in the course of commercial activities.

6. **Limitations** The general limitation in Part 1 is that you can collect, use or disclose personal information only for purposes that a "reasonable person" would consider "are appropriate in the circumstances" (even if the individual consents).

You cannot, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of information beyond what is required to fulfil your explicitly specified and legitimate purposes.

Finally, you must not obtain consent through deception.

7. **Accuracy** Personal information must be as accurate, complete and up-to-date as is necessary for the purposes for which you are going to use it. The degree of accuracy depends on the circumstances: minimize the possibility that “inappropriate information” is used to make a decision about the individual.

Keep information up-to-date if it is being used on an ongoing basis; but do not routinely update information if it is not necessary to do so to fulfil the purposes for which it was originally collected.

8. **Safeguards** Protect personal information by safeguards “appropriate to the sensitivity”, against loss or theft and against unauthorized access, disclosure, copying, use or modification. Safeguards may be physical (e.g., locked cabinets, restricted access to offices), organizational (e.g., security clearances) and technological (e.g., passwords, encryption).

Your responsibility extends to personal information you have transferred to a third party for processing; you must, by contract or other means, make sure that there is a comparable level of protection during such processing.

The same level of care applies to disposing of or destroying personal information, so that unauthorized parties do not get access to it.

9. **Access** Individuals have the right to be informed of the existence, use and disclosure of their personal information, and to be given access to that information so that they can challenge its accuracy and completeness and have it amended. This means you have to be able to identify what information you have about particular individuals, so you can make it available if they ask.

10. **Retention and destruction** Personal information must be retained only as long as necessary to fulfil the purposes for which it was collected; again, this means that you have to be able to identify what information you have about particular individuals, so that you can destroy it when you no longer need it.

11. **Challenging Compliance** Individuals have the right to challenge not only the accuracy and completeness of the personal information you hold about them, but also your level of compliance with the requirements of Part 1 and the Code.

12. **Accountability** You must designate a particular individual as being accountable for your compliance, and complaints and inquiries will be addressed to that person. You must designate a particular individual as being accountable for your compliance, and complaints and inquiries will be addressed to that person.

13. **Enforcement** Part 1 is administered by the federal Privacy Commissioner. When disputes arise, individuals and organizations will be encouraged to resolve them by negotiation, and if necessary mediation and arbitration. The Commissioner has broad powers to investigate and report on complaints, and to audit your information practices.

The Commissioner’s report itself is not legally enforceable, but once it is delivered the individual can make an application to the Federal Court, which has broad powers to make corrective orders and award damages (including punitive damages).

@ @ @

If you would like to know more about this legislation in general (or, in Québec, the existing personal information laws of that province), please do not hesitate to call or write to the indicated contact in the most convenient of the offices of Borden Ladner Gervais LLP shown below. BLG is happy to provide general information as a service to Equifax clients, but cannot provide legal advice on specific fact situations without a lawyer-client retainer for that purpose; any such retainer would be for your account, not that of Equifax Canada Inc.

Vancouver: Roger McConchie, (604) 640-4080, rmcconchie@blgcanada.com

Calgary: Michael Massicotte, (403) 232-9602, mmassicotte@blgcanada.com

Toronto: Brian Keith, (416) 367-6217, bcketh@blgcanada.com

Ottawa: Peter Doody, (613) 787-3510, pdoody@blgcanada.com

Montreal: Thomas Davis, (514) 954-3133, tdavis@blgcanada.com