



OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

**GUIDELINES FOR
DATA SERVICES CONTRACTS**

OIPC GUIDELINE 01-02

Date: May 8, 2003
(Replaces: November 14, 2001)

1.0 PURPOSE OF THIS DOCUMENT

These guidelines of the Office of the Information and Privacy Commissioner for British Columbia (“OIPC”) are for use by public bodies, including any provincial government ministries, that contract out:

- the processing or storage of information that includes personal information;
- the operation or management of computerized systems containing personal information; or
- services involving the collection, use or disclosure of personal information.

Despite the possible cost-savings or other benefits of contracting out such information services, public bodies must not forget the risks to privacy that can arise where personal information is being collected, used, disclosed or managed by an outside service provider who is not familiar with, or equipped to meet, the statutory obligations regarding personal information in Part 3 of the *Freedom of Information and Protection of Privacy Act* (“Act”). (A copy of the Act is found at www.oipc.bc.ca/legislation/FOI-ACT.pdf.) Privacy risks include use or disclosure of personal information by unauthorized personnel, compromised integrity of personal information, accidental disclosure of personal information, improper use or disclosure of personal information and improper retention or secondary use of personal information. These guidelines are intended to address risks to privacy that may arise in the contracting out situations described above.

These guidelines acknowledge that a public body cannot, by contracting out, relieve itself of its privacy obligations under Part 3 of the Act. To maintain public confidence in the public body’s handling of personal information, and to ensure compliance with the Act, each contract for personal information services should require the service provider to comply with the Act and any privacy practices specified in or under the contract. It is also important for the public body to monitor performance, and enforce the agreement, including by conducting periodic audits as provided in the contract.

The OIPC recognizes that implementation of these guidelines will have cost implications for the public body. It is within a public body’s discretion to decide which of these guidelines should be implemented in any such arrangement, and how, but it must be remembered that these guidelines will in turn guide the OIPC in assessing any contracting-out arrangement when investigating whether the public body has met its obligations under Part 3 of the Act. For an example of such an investigation, see Investigation Report 01-01, at <http://www.oipc.bc.ca/investigations/reports/IR01-01.pdf>.

These guidelines have benefitted from study of publications of the Office of the Information and Privacy Commissioner of Ontario, whose efforts are gratefully acknowledged.

This document is for information only. It does not provide legal or other advice. These guidelines do not constitute a decision or finding by the OIPC respecting any matter within the jurisdiction of the Information and Privacy Commissioner under the Act. These guidelines do not affect the powers, duties or functions of the Information and Privacy Commissioner respecting any complaint, investigation or other matter under or connected with the Act and the matters addressed in this document.

2.0 GENERAL

2.1 Definitions – These guidelines deal with contracting out arrangements that involve “personal information” as defined in the Act. The Act defines “personal information” as “recorded information about an identifiable individual”. This will *include* the following types of personal information:

- (a) the individual's name, address or telephone number,
- (b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,
- (f) information about the individual's health care history, including a physical or mental disability,
- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinions about the individual, and
- (i) the individual's personal views or opinions, except if they are about someone else.

Personal information is “recorded information” *of any kind*, so long as it is “about an identifiable individual”. This means that, even if someone’s name or other identifier is not part of the personal information, the individual the information is about may be “identifiable”, making the information “personal information”. If personal information is involved, the public body must comply with Part 3 of the Act in collecting, using, disclosing and securing the personal information and this extends to the contracting-out arrangement.

The Act defines the term “record” as follows:

“**record**” includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records;

A “record” is *any* physical, electronic or other medium in or on which personal information is recorded. The Act’s definition says that a “computer program” is not a

record. This is intended to protect software and does not limit the Act's application to personal information that is in electronic form.

The Act's definitions of personal information and record should be incorporated into any contract for personal information services.

2.2 Privacy Impact Assessment – A public body should carry out a privacy impact assessment (“PIA”) before it makes the final decision to contract out personal information services. A link to the model PIA tool jointly developed by the OIPC and the Corporate Privacy and Information Access Branch of the Ministry of Management Services is found at http://www.msar.gov.bc.ca/foi_pop/manual/forms/pia.doc. At present, it is mandatory for provincial government ministries to carry out PIAs.

2.3 Involving Privacy Staff in the Contract Process – A public body should involve its privacy staff in preparing tender documents or request for proposal (“RFP”) documents. Access and privacy staff should also be involved in the actual contract process as well. The RFP or tender documents should make it clear to prospective contractors what the Act requires and should alert them, in as much detail as practicable, to the specific privacy duties and obligations they will be required to meet. This will ensure that bids or proposals address the privacy requirements at the outset. Ideally, a public body that contracts out personal information services frequently should create, and send to prospective service-providers, standard-form privacy provisions for RFPs and contracts.

3.0 GUIDELINES FOR CONTRACT TERMS

Each contract should include provisions addressing the matters discussed below. A public body also should refer to any available sources for current, generally-accepted best practices and consider their implementation through the contract, even if they are not mentioned here.

The complexity of some arrangements may require further provisions than are contemplated by the following guidelines. Some contracts may require fewer controls than the following guidelines contemplate.

Much depends on the circumstances, mainly the nature of the personal information in question and the nature of the services to be provided to the public body. For example, if the personal information is sensitive information (such as health information) and the services will involve collection, use and disclosure of such information (as opposed to simple storage or archiving of information), the service agreement should reflect these guidelines.

In more straightforward cases (such as where the information is not sensitive or the services do not involve collection, use or disclosure of personal information), the service contract may be more basic. Standard-form privacy protection clauses of that kind can be found through the following Ministry of Management Services website: http://www.msar.gov.bc.ca/FOI_POP/PPS/default.htm. That website contains links to

a privacy protection contract schedule designed for provincial government ministries and a schedule designed for use by other public bodies.

3.1 General Provisions About Application of the Act – This section sets out the general contract provisions that should be included in contracts.

1. The contract must incorporate the Act’s definitions of “personal information” and “record”.
2. The contract must state that the public body is only transferring *physical custody* of personal information to the contractor, not *control* of that information, and must state that authority over personal information use, disclosure, access, destruction and integrity remains with the public body. The contract should state how the public body can exercise that control (*e.g.*, by giving a notice to the contractor that requires the contractor to do what is specified in the notice).
3. The contractor must be required to comply with the fair information practices in Part 3 of the Act and to implement appropriate security measures required under the contract.
4. The contractor must be required to appoint a knowledgeable senior person within its organization to be responsible for privacy compliance and to be the contact for such issues. That person must have the necessary authority to do these things. The public body must be required to do the same.
5. The public body should carefully consider whether the contractor should be allowed to sub-contract any services under the contract. If sub-contracting is allowed, only qualified sub-contractors should be permitted. The contractor should be required to ensure that any sub-contract requires the sub-contractor to comply with the privacy provisions of the contract between the contractor and the public body. The public body should consider requiring the contractor to get the public body’s express, written approval of sub-contract provisions before the sub-contract is signed, with the public body having the discretion to refuse approval if it reasonably considers the proposed sub-contractor does not have the experience and capacity to perform the sub-contract.
6. If the contract allows the contractor or any subcontractor to have access to personal information, the contract must expressly specify how, why and when access is permitted.

3.2 Personal Information Storage and Access – The contract should contain the following provisions dealing with the storage of, and access to, personal information.

1. The contractor should be required to:
 - (a) take a physical inventory, at least annually, of all records containing personal information, to identify any losses;

- (b) ensure that records are not removed from storage premises without appropriate written authorization;
- (c) use physically secure areas for the storage of records and restrict access to authorized personnel;
- (d) ensure that access to documentation about computer systems that contain personal information is restricted to authorized personnel;
- (e) ensure that users of a system or network that processes personal information are uniquely identified and that, before a user is given access to the system or personal information, their identification is authenticated each time;
- (f) implement procedures for *identification* and *authentication*, which include:
 - (i) controls for the issue, change, cancellation and audit-processing of user identifiers and authentication mechanisms;
 - (ii) ensuring that authentication codes or passwords:
 - (A) are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code;
 - (B) are known only to the authorized user of the account;
 - (C) are pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition;
 - (D) are no fewer than 6 characters in length;
 - (E) are one-way encrypted;
 - (F) are excluded from unprotected automatic log-on processes; and
 - (G) are changed at irregular and frequent intervals at least semi-annually;
- (g) maintain and implement formal procedures for terminated employees who have access to personal information, with prompts to ensure revocation or retrieval of identity badges, keys, passwords and access rights;
- (h) position system display units and hardcopy documents, or equip them with protective material, so that any personal information being displayed or processed cannot be viewed by unauthorized persons;
- (i) implement automated or manual controls to prevent unauthorized copying, transmission or printing of personal information;

- (j) design and implement a public body-approved automated, always-on auditing system, that is available to the public body for monitoring access to and the use of personal information in the custody of, or managed by, the contractor;
 - (k) ensure that, bearing in mind the OIPC's *Guidelines for Audits of Automated Personal Information* OIPC Guideline 01-01 <http://www.oipc.bc.ca/publications/advice/audit-3.pdf>, the audit system referred to in 1(j) creates audit trails that automatically:
 - (i) record the identity of anyone who accesses, views, alters, deletes or uses a record containing personal information for any purpose, or attempts to do any of those things, and records the date and time of any such actions; and
 - (ii) flag accesses, or access attempts, that fall outside of set criteria (*e.g.*, access outside regular working hours); and
 - (l) implement control procedures to ensure the integrity of the personal information being stored, notably its accuracy and completeness.
2. The contractor must store personal information on agreed-upon media in accordance with prescribed techniques that store the personal information in a form that only authorized persons may access. These techniques may include translating the personal information into code (*encryption*) or shrinking or tightly packaging the personal information into unreadable form (*compression*).
 3. The contract should specify the location where personal information will be stored.
 4. The contractor must ensure that it stores backup copies of records off-site under conditions which are the same as or better than originals.
 5. The contractor should be required to securely segregate personal information from information owned by others (including the contractor), including by installing *access barriers* to prevent information elements from being associated (including compared or linked, based on similar characteristics) with other information, including:
 - (i) separate storage facilities for the public body's personal information;
 - (ii) authorization before a person is granted access to computers containing such personal information; and
 - (iii) entry passwords and the employment of public key encryption/smart card technology where practicable.
 6. The contractor must be required to ensure the integrity of personal information stored, processed or transmitted through its system or network.

7. The contractor should be required to take all reasonable steps to ensure personal information is accurately recorded, complete, updated and not deleted or altered except as directed by the public body in writing.
8. The contract should establish a process by which individuals can access their own personal information, in the custody of the contractor, through an access request under, and as permitted by, the Act.
9. The contract should require the contractor to co-operate with, and assist in, any public body investigation of a complaint that personal information has been used or disclosed contrary to the Act or the contract.
10. The contract should give the public body a right of access to the contractor's premises to recover any or all of its records and for auditing purposes to ensure contract compliance.

3.3 Enforcing Privacy and Security – It is crucial that the public body have meaningful, practical methods to monitor and enforce compliance.

1. There should be significant, effective remedies and penalties for violation of contract terms and conditions governing personal information. This should include processes for dispute resolution, and for determining appropriate remedies, if contractors or sub-contractors breach the contract.
2. The contract should require the contractor to ensure that employees engaged in performance of the contract, and any sub-contract, sign a privacy and confidentiality agreement which includes a clause specifying that discipline, up to and including termination of employment, may result if an employee, without authority, accesses, uses, discloses or disposes of personal information contrary to the contract. The contractor should be required to regularly refresh this agreement with employees.
3. The contractor should assume full responsibility for any negligent or wilful act or omission of any of its employees or sub-contractors respecting unauthorized access, use or disclosure of personal information. The contractor should be required to indemnify the public body for any liability the public body incurs as a result of unauthorized access, use or disclosure.
4. The contractor should be required to comply with the public body's retention, destruction and archival storage of personal information. At the very least, the contract should stipulate that the contractor must not destroy personal information unless the public body has identified the relevant personal information in writing and expressly directed its destruction.
5. The contractor should be required to return personal information to the public body, or destroy it, on termination of the agreement.

6. The contractor must receive personal information from the public body and disclose it only to the appropriate public body, or to agents authorized expressly in writing by the public body that provided the personal information, and then only through approved processes.

3.4 Encouraging Good Privacy Practices – Ongoing education and training are key to proper privacy protection. The contract should therefore include provisions addressing the following points.

1. At the start of the contract's term, and periodically during the term, the public body should provide appropriate guidance on the Act and its requirements to the contractor and its employees.
2. The contractor should be required to provide appropriate and ongoing training on the Act and the contract, and their requirements, to its employees and, where practicable, to approved sub-contractors and their employees. The contractor should, at a minimum, be required to include in any sub-contract provisions that implement paras. 3.3.1 through 3.3.3, above (and such other of these guidelines as are applicable).

3.5 Other Restrictions – The contract should also deal with the following added matters.

1. The contract should prohibit the contractor from sharing, matching or mining (or otherwise combining or manipulating personal information) except as agreed-to in writing, in advance, by the public body and subject always to what is permitted under the Act. Any current or new activities of these kinds that are agreed to by the parties must be subject to a new PIA undertaken by the contractor or sub-contractor in consultation with the public body.
2. The contract should prohibit the contractor from withholding personal information to enforce payment by the public body or in any contract dispute.