Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Guidance Document:

Taking Privacy into Account Before Making Contracting Decisions

Issued to federal government institutions by the Treasury Board of Canada Secretariat

Canada

Catalogue No. BT22-106/2006E-PDF
ISBN 0-662-43030-1

This document is available on the Treasury Board of Canada Secretariat Web site at www.tbs-sct.gc.ca

This document is also available in alternate formats on request.

Table of Contents

1. Introduction

Purpose of this document

This guidance document is intended to provide advice to federal government institutions whenever they consider contracting out activities in which personal information about Canadians is handled or accessed by private sector agencies under contract.

The document was developed in response to privacy risks associated with the potential exposure of Canadians' personal information to U.S. authorities under the *USA PATRIOT Act.*

Why this document was developed

It is not uncommon for a federal government institution to contract out the management of a program or service involving personal information about Canadians to a company based in Canada, the U.S., or another country. When information is stored or accessible outside of Canada, however, it can be subject not only to Canadian laws but also to the laws of the other country.

One such law is the *USA PATRIOT Act*. The Act permits U.S. law enforcement officials to seek a court order allowing them to access the personal records of any individual for the purpose of an anti-terrorism investigation without informing individuals or agencies that such disclosure has occurred. In theory, as a result of government contracting activities, U.S. officials could access information about Canadians through U.S. firms or their affiliates, even if the data is located in Canada.

Although the risk of U.S. authorities using the *USA PATRIOT Act* in this way is minimal, it nevertheless exists. This has highlighted the need for special considerations with respect to government contracts involving personal information in order to mitigate such privacy risks.

The significance of the *USA PATRIOT ACT* has been summarized by the Privacy Commissioner of Canada, Jennifer Stoddart:

> The concerns raised about the impact of the *USA PATRIOT Act* on the privacy of personal information about Canadians are really part of a much broader issue—the extent to which Canada and other countries share personal information about their citizens with each other, and the extent to which information that has been transferred abroad for commercial purposes may be accessible to foreign governments. The enactment of the *USA PATRIOT Act* may simply have served as the catalyst that brought these issues to the fore.

The Government of Canada takes the issue of privacy very seriously. It supports the assessment of the Privacy Commissioner of Canada that the *USA PATRIOT Act* highlights the broader issue of personal information about Canadians becoming accessible to any foreign government.

2. About the Guidance Document

Overview

The guidance document was developed by the Treasury Board of Canada Secretariat (the Secretariat) after consultation with federal government privacy and contracting experts. It is strongly recommended that institutions follow the advice offered in this document in order to mitigate privacy risks.

Each institution is responsible and accountable for any personal information under its care. Personal information is defined in section 3 of the *Privacy Act* as "information about an identifiable individual that is recorded in any form".

The document provides federal government officials involved in contract management with an overview of the possible strategies available to protect personal information and addresses privacy issues in contracting out that may be associated with the *USA PATRIOT Act* or other similar foreign legislation.

Benefits of using the document

The guidance document will help you in two ways:

1. Firstly, it provides upfront assistance to government officials before the commencement of a contracting process in which personal information may be handled under a proposed contract. This first phase, covered in steps 1 and 2 (under "Steps to Follow"), will guide you in making an informed decision on whether an outsourcing contract is appropriate or not or, in cases where a contract is already in place, whether the contract should be renewed.

2. Secondly, once a decision has been made to proceed with a contract, steps 3 to 5 will provide guidance on clauses and wording that can be considered for requests for proposals (RFP), statements of work (SOW), and contracts, all of which are designed to mitigate privacy risks.

Who should use the document?

The guidance document contains general policy advice for all federal government institutions that are subject to the *Privacy Act.* This includes approximately 170 federal departments, agencies, and Crown corporations.

The document is therefore useful for all federal government employees involved in program and service development and delivery that includes the collection, use, disclosure, retention, and disposal of personal information.

The *Privacy Act* is available on the Web site of the Department of Justice Canada: http://laws.justice.gc.ca/en/P-21/index.html.

3. Considerations

Use the document within a broader context

This guidance document is meant only as a guide and government institutions should not rely solely on it in the preparation of a contract or any other document. The advice contained in this document is not intended to be read in isolation, but in conjunction with existing government policies and procedures for procurement. Institutions are encouraged to consult with their legal and privacy officials to ensure that no misinterpretation occurs and to determine appropriate privacy measures that apply to their particular circumstances.

It is important to remember that there is no universal approach, and potential contracting situations must therefore be reviewed on a case-by-case basis.

Appropriate provisions and consultation

In accordance with the Treasury Board *Contracting Policy*, contracting authorities are responsible for ensuring that appropriate provisions for the protection of government information are included in procurement documents.

Contracting Policy
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/Contracting/siglist_e.asp

In cases where personal information may be handled under the terms of a contract, institutions should consider the inclusion of appropriate clauses to protect personal information as a shared responsibility.

Program officials should bring plans to contract out the handling of personal information to the attention of procurement officials and, when necessary, consultations should be undertaken with the institution's privacy and legal officials.

Consideration of contract and security requirements

Although the main focus of this guidance document is on addressing privacy concerns and risks, the advice contained in the document can be applied to other protected or classified information, as defined in the *Government Security Policy* (GSP), that may be handled under contracts.

The guidance document is intended to complement the government's existing contractual and security requirements and advice already in place to safeguard personal and other sensitive information.

Such requirements and advice are contained in other government publications, including the following:

Standard Acquisition Clauses and Conditions
http://sacc.pwgsc.gc.ca/sacc/contents-e.jsp

The Industrial Security Manual
http://www.ciisd.gc.ca/ism/text/ch1-e.asp

Government Security Policy and its accompanying standards
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/siglist_e.asp

Issues related to the security and confidentiality of classified information should be addressed in collaboration with contracting officials and the institution's security officers. Contracting authorities are expected to include pertinent provisions in the RFP and final contract to address security requirements and to ensure that any subcontracts that might be permitted also contain similar clauses.

Where required, a Security Requirements Check List (SRCL) form must be filled out and consultations undertaken with the Canadian and International Industrial Security Directorate at Public Works and Government Services Canada (PWGSC).

A threat and risk assessment may also be required when protected or classified information (which may include personal information) will be accessed or handled under contract.

Institutions must implement the GSP when sharing Government of Canada information and, more specifically, the GSP procedures for safeguarding and storage of information should be read in conjunction with this guidance document.

Section 10.1 of the GSP *Operational Security Standard on Physical Security* is of particular relevance and can be found at the following address:
http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/osps-nosm1_e.asp#preamble

4. Getting Started

Building trust

From a policy perspective, the term “privacy” means more than just ensuring security and maintaining confidentiality of personal information by protecting against misuse or wrongful disclosure. Privacy also relates to the trust relationship that is built between individuals who provide personal information and those who collect it. It means providing individuals with a comfort level with respect to government handling of their personal information.

Privacy considerations are particularly relevant when considering contracts that may involve transferring personal information and data across borders. In such instances, the personal information is subject to foreign laws and thus potentially accessible.

The steps outlined in the next section are intended to assist program officials and privacy experts, in consultation with their legal counsel, to determine whether to enter into contracts involving the handling of personal information or, in some cases, to revisit the decision to contract if it has been determined beforehand.

Making an informed decision

As part of good management practices, federal institutions consider the costs and benefits of contracting for a service. All contracting decisions, including those that will involve personal information, take a number of important factors into account, such as the costs of program delivery and level of service, before entering into the contract.

The first step in the process is to identify any privacy risks. More information on this initial phase and other critical steps is provided in Step 1.0 and in Appendix A.

To identify all of the appropriate privacy and access to information measures government officials should take into account during the framing of a contract that involves personal or sensitive information, refer to Appendix B, “Privacy Protection Checklist. ” The checklist is a practical tool that guides the project authority through a series of privacy and

access-to-information questions that ensure appropriate control, collection, use, disclosure, subcontracting, and other key factors in designing a contract.

The make-or-buy decision is based upon privacy, security, and other key business case considerations, such as quality and speed of service, the feasibility of carrying out the program or service in-house, the need for specialized expertise, trade obligations, and costs.

Making the procurement decision involves a multi-faceted analysis and should involve consultations with contracting, privacy, and other relevant officials within the government institution. Even when highly sensitive personal information is involved, appropriate privacy mitigation strategies, such as contract clauses, can be implemented so that the level of overall risk is reduced before contracting is initiated.

This guidance document is intended to promote a balanced approach and forms the basis of a well-informed decision on whether or not to contract out.

If a decision is made to proceed with a contract, Step 4.0 contains suggested wording for contract clauses that should be built into the contractual agreement to enhance privacy protection and reduce risks.

5. Steps to follow

Steps 1 to 2, Pre-contract

Step 1.0: Contracts involving personal information

Once it is determined that personal information (as defined in the *Privacy Act*) about identifiable individuals will be involved in the program or service, and that a contract is being considered as an option, the institution's analysis should include the following:

1.1 compliance with the *Privacy Act* and Treasury Board privacy policies;

1.2 an invasion-of-privacy test; and

1.3 a Privacy Impact Assessment (PIA) or a Preliminary PIA (PPIA), if not already completed.

1.1 The *Privacy Act* and Treasury Board Privacy policies

When federal government functions or services are performed under contract by third parties, care must be taken to ensure that the government continues to fulfil its privacy obligations. The personal information must be managed so that the government institution conforms to the fair

information practices embodied in sections 4 through 8 of the *Privacy Act*, the *Privacy Regulations*, the Treasury Board policy on *Privacy and Data Protection* and its *Privacy Impact Assessment Policy*. In particular, the institution must have the authority to collect the personal information that will be involved in the contract and the information must, in accordance with section 4 of the Act, relate "directly to an operating program or activity of the institution."

1.2 Invasion-of-privacy test

The invasion-of-privacy test was first developed for the Treasury Board manual, which contains guidelines for the policy on *Privacy and Data Protection*. The test suggests that institutions consider three interrelated risk factors:

- the sensitivity of the personal information, including whether the information is detailed or highly personal (e.g., health information), and the context in which the information was collected;
- the expectations of the individuals to whom the personal information relates (including the assurance that their information will be shared only on a need-to-know basis); and
- the potential injury if personal information is wrongfully disclosed or misused, including the potential for identity theft or access by foreign governments.

The above privacy considerations will assist institutions in identifying potential risks with respect to the proposed program delivery instrument that should be mitigated as part of the contracting process. For additional guidance on this matter, please refer to Appendix A, "Invasion-of-privacy Test."

1.3 *Privacy Impact Assessment Policy*

Institutions subject to the *Privacy Act* are also subject to the *Privacy Impact Assessment* (PIA) *Policy*: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp.

Under the PIA Policy, institutions are required to consider conducting a PIA when any new program or service involves the collection, use, or disclosure of personal information or when any significant change is made to an existing program or service. This would include the contracting of a program or service to the private sector. The deputy head of the institution is responsible for determining whether initiatives warrant the conduct of PIAs. In some instances, where institutions do not yet have detailed information required for a comprehensive assessment or where a change to a program or service (or the contracting thereof) is not considered so significant as to warrant a full PIA, it may be appropriate to conduct a preliminary PIA.

Step 2.0: Assess privacy risks against other considerations

Depending on the circumstances at the institution, there are a number of other factors that could be taken into account at this stage. The privacy risks identified and assessed in Step 1.0—in particular, the sensitivity of the information and the amount of control that the service provider has over the information—will need to be weighed against the following factors before reaching a final decision.

2.1 Laws of foreign jurisdictions

As part of doing business in circumstances that may allow the application of laws of foreign jurisdictions (e.g. subcontracts, change of ownership), institutions should give consideration to whether contracts or operations under contracts can be negatively affected by the foreign jurisdiction's economy, political reality, laws, or legal system. In some instances, these differences in a foreign environment may give rise to questions with respect to possible privacy risks.

Foreign search and seizure laws, for example, may require companies that are based within their jurisdiction, or that have ties to companies within their jurisdiction, to disclose information that is either under their control or to which they can obtain access, including information held under a contract or arrangement. The following scenarios provide examples of how such laws could potentially apply if Canada enters into a contract with a company:

Scenario A: Contract with a company operating in Canada and not in any foreign country

A company operating only in Canada that maintains personal information only in Canada is subject to Canadian legislation. There is an indirect risk of access if, under the terms of the contract, the Canadian company (the contractor) has the authority to subcontract and thus may subcontract with companies that are based in a foreign country or have links to foreign commercial organizations.

Scenario B: Contract with a company operating both in Canada and in a foreign country

An order pursuant to a foreign law could indirectly apply. A foreign-based company could be required to disclose personal information to which it has access or can obtain access, including information held by its Canadian affiliate under contract. Depending on the nature of the foreign legislation and the ease of access to the records by the foreign-based company, the Canadian affiliate may not be made aware of an order to produce information.

Scenario C: Contract with a company operating in a foreign country

Commercial organizations operating in a foreign country that hold personal information about Canadians in that country must comply with the laws of the foreign country. A foreign-based company could be required to produce personal information to which it has access or can obtain access as a result of a contract or arrangement with a Government of Canada institution.

The above examples could apply to any foreign jurisdiction with laws that can compel the production of information from companies operating within their borders. Note that it would be much more difficult for most foreign governments to target specific personal information that may be held by a company under the terms of a contract with the Canadian government than it would be to request information through an existing bilateral agreement. In considering the possible use of the *USA PATRIOT Act* by U.S. law enforcement to get information about Canadians, the Privacy Commissioner of Canada stated the following:

> . . . US government agencies can rely on other established procedures to obtain information about Canadians that is held by government or the private sector in Canada. Longstanding information sharing agreements between security and law enforcement agencies in both countries, and the mutual legal assistance process, are the most likely vehicles for obtaining access to information held in Canada.

It should be noted that the *Personal Information Protection and Electronic Documents Act* (PIPEDA) or substantially similar provincial laws (in place only in British Columbia, Alberta, and Quebec) regulate the privacy practices of commercial organizations operating in Canada. None prevents contracting involving personal information, but they do require that Canadian-based contractors include privacy-protective clauses in any subcontracts.

2.2 Analysis of possible application of international trade agreements

Before deciding whether or not to contract out for the handling of personal information, institutions should determine whether international trade agreements apply to the proposed procurement (Appendix C provides a brief overview of some key trade agreements). If such agreements apply to the procurement, the Government of Canada must ensure that its trade obligations are met and that requests for proposals are consistent with these obligations.

In practical terms this may mean that, in some cases, government institutions would not be able to require that information be retained in Canada. The applicability of trade agreements is therefore an important determination and may be influential in decisions to initiate a particular procurement approach or to examine alternatives.

Government officials should consult with legal advisors to determine whether international trade agreements are applicable.

Steps 3 to 5, Contracting

Step 3.0: Building privacy into contracts

If the decision is to proceed with a contract, institutions should ensure adequate privacy protection is included in contract documents, as outlined in Steps 3.0 and 4.0. Government institutions can employ a variety of tools in the procurement process to ensure that any resulting contract will include adequate privacy protection. The evaluation criteria, the SOW, as well as other provisions of the RFP are among the most effective vehicles for ensuring upfront protection of personal information. The initial design and drafting of such procurement documents should establish overall privacy protection strategies and should produce the key provisions for ensuring appropriate privacy protection through contracts. All effective contracting solutions must take implementation costs into consideration.

3.1 Request for proposals / statement of work

One of the most fundamental risk considerations when establishing contracts that involve the handling of personal information is to ensure that the information will be collected, used, retained, and disclosed only for the purposes specified in the contract and that it will be accessible only to authorized individuals (on a need-to-know basis) for those purposes. Depending on the arrangement, this may require additional contractual safeguards, especially where the information is being accessed or held by a foreign-based contractor or a contractor with ties to a foreign jurisdiction.

Privacy risks must be considered at this early stage of the procurement process. It is imperative that all potential bidders or contractors are aware of any specific requirements associated with the performance of the contract at the RFP stage since such requirements will affect costs. The decision to include specific provisions in the RFP or SOW should be based on overall risk considerations, including potential privacy impacts and the need for contract clauses that mitigate risks.

Any restrictions related to the access, use, and storage of personal information must be reflected in the procurement documents, including the RFP or the SOW.

At the RFP or SOW stage

Based on the results of the invasion-of-privacy test and other risk factors, if it is determined that the risk level is relatively high, institutions may consider the following:

- In cases where international trade agreements do **not** apply, is there a requirement that the work must be conducted and data retained in Canada or Government of Canada facilities (e.g. foreign embassies, military facilities abroad)?
- Is there a requirement for the contractor to segregate the government information or database from other information?
- Is there a requirement for the provision of an information management and security plan by the contractor (i.e. documentation that details exactly how the information will be treated over its life cycle and how its security will be ensured)?
- Is there a requirement to obtain assurances that the bidder can meet the requirements of the contract or demonstrate certain qualifications or certification before the RFP process (i.e. are bidders pre-qualified based on their ability to manage personal information)?
- Will the contractor be required to provide or make use of specific systems, equipment, or records with respect to the privacy and security of the government information?
- What will be available to the contractor (e.g. facilities, systems, records, databases)?
- Will the contractor be required to provide and maintain a list of personnel who will be authorized to access the government information or databases under the contract?
- Will the Government of Canada have control of the information, and will the responsibilities for the handling (i.e. collection, use, storage, disposal, and disclosure) of the information be stipulated?
- Will the contractor be required to maintain audit trails and report on all access to and disclosures of the government information or databases?
- Will there be a need to demonstrate proof of government-authorized destruction?

Note: All contracts for services have an SOW or a description of requirements, which clearly describes the work to be carried out, the objectives to be attained, and the time frame. The SOW will be part of the RFP and the contract.

Where privacy risks are considered high, government institutions may wish to specifically evaluate the bidders' privacy protection strategies. If bidders will be required to produce a privacy management plan as part of the contract, government institutions may request that such plans be included in response to the RFP as part of the bidder's submission for evaluation during the procurement process. The federal institution could then assess such plans and give them appropriate weight in the evaluation criteria.

Step 4.0: Specific considerations for RFPs and contracts involving personal information

Important note: The *Standard Acquisition Clauses and Conditions Manual* (SACC), published by PWGSC, may provide adequate protection in many cases where contractual arrangements

involving personal information are being made. It is therefore imperative that government officials consult their legal services and privacy officials regarding the application of additional or revised contractual language on a case-by-case basis.

The following are some considerations related to the protection of personal information that will be useful in mitigating the risk of possible unauthorized disclosure to foreign governments and in ensuring appropriate care and monitoring of contracts involving personal information. In some cases, these considerations for suggested clauses may already be requirements under other contracting and security policies, directives, and guidelines that currently apply to most institutions subject to the *Privacy Act*. The intent of including the suggestions below is not to limit the requirements for privacy clauses but to point out that the following matters are of particular significance and should be considered in RFPs and contract clauses.

4.1 Establish control

It is important that the nature of the relationship between government institutions and contractors and their respective roles and obligations be clearly specified in contractual arrangements. A government institution cannot collect personal information unless it is directly related to an operating program or activity of the institution.

The institution must examine the scope of its legal authority for a program or activity. Once the authority is established, contracts for the management of government programs and services should include provisions to ensure that the government institution maintains control over personal information or other records that are transferred to the contractor and, where appropriate, over information collected, created, obtained, or maintained by the contractor in fulfillment of the contract. Establishing control is necessary to enable the contracting institution to comply with its statutory obligations under the *Privacy Act* and the *Access to Information Act*. This is of particular importance when highly sensitive information is to be stored or processed in a foreign country by a foreign-based company, subsidiary, or third party, such as a subcontractor or agent. Government institutions can establish control by defining the institution's proprietary rights to the information in the contract, including the institution's right to obtain the records upon request.

In addition, the government has a duty to include other specific privacy protection provisions in the contractual agreement to ensure that the contracting out of government programs and services does not result in a reduction of privacy protection. There may be instances where federal institutions subject to the *Privacy Act* enter into contractual agreements with organizations in the private sector that are subject to other legislative privacy requirements at the provincial or federal level, such as PIPEDA. Federal institutions faced with this kind of scenario

should, in consultation with their institution's legal and privacy officials, conduct a thorough legislative and policy analysis of the requirements of both laws and develop contractual clauses in keeping with the more stringent privacy principles or standards of the two laws.

4.2 Confidentiality use for purposes related to the contract

Institutions should ensure that provisions are in place to limit access (including unauthorized access) to, or the ability to obtain the sensitive personal information for purposes not related to the contract, including any disclosure or access by a foreign-based parent company, other affiliates, or third parties, such as subcontractors or agents that are not directly named in the primary contract or arrangement. In cases where sensitive personal information is being accessed, government institutions should either include a requirement for the contractor to specifically identify and designate all contractor employees who will have access to the personal or proprietary data, or identify positions of employees who will have access. This would assist in revealing any incidents of unauthorized access, especially where audit trails are used.

4.3 Audits required or permitted (including verification of tracing and audit trails)

In addition to standard audit provisions, when sensitive personal information is being accessed, institutions should consider a requirement to stipulate that the supplier or service provider maintain specific information to enable the conduct of informational audits. Audits of security and privacy, for example, will require maintenance on the part of the contractor of some form of audit trail (electronic or paper form) to demonstrate that those who accessed information had the proper authority to do so.

4.4 Segregation of information

The contracting authority should consider including provisions to ensure that mechanisms are in place requiring that all sensitive personal information disclosed to a contractor by the Government of Canada, or collected or created pursuant to a contract or arrangement with the Government of Canada, is separated or segregated from other records or company data holdings. Institutions should qualify the nature of the segregation, which may include the physical separation of data (e.g. data held on a magnetic tape), the logical separation of data (e.g. record or user ID), or a combination of both physical and logical separation.

Note: References to segregation of information in the contract must be consistent with the terms established in the RFP and SOW, as well as the PWGSC SACC manual.

4.5 Conditions for disclosures unrelated to the contract

The government institution should consider placing specific requirements for the contractor to account for and obtain prior approval of all disclosures of sensitive personal information unrelated to the contract (see 4.2, “Confidentiality use for purposes related to the contract”).

4.6 Inspection

Where a government institution establishes control (see 4.1, “Establishing control”), it may also wish to put in place broad powers to inspect the contractor’s premises when sensitive personal information is involved. Past contracts related to records disposition have highlighted the importance of inspecting facilities and the actual work that is being conducted under contract. It is important that government institutions verify (not necessarily through audit) that the work is being conducted in the manner specified in the SOW and respects the conditions outlined in the RFP. If, for example, the RFP and SOW have particular requirements (technical or other), institutions may wish to allow Canada the right to inspect the work to ensure that the service provider is conducting the work in accordance with the specifications outlined in the RFP, the SOW, and the contract.

4.7 Notification of breach

Given the government’s obligations to protect personal information under its control, the responsibility to ensure confidentiality and the accountability for breaches should be extended to any contractor that is handling personal information on behalf of an institution. If a contractor is deemed to be at fault for a breach of confidentiality, the contractor should be prepared to accept the responsibility for a wrongful disclosure of personal information, the costs associated with the appropriate notification of the individuals whose information has been disclosed, and the possibility of termination of the contract. Institutions should specify that, immediately after the contractor becomes aware of a breach of confidentiality, the contractor must notify the government institution forthwith that the breach has occurred.

4.8 Notice of subcontractor and subcontractor obligations

Where appropriate, the government institution should carefully consider whether the contractor should be allowed to subcontract any services under the contract. If subcontracting is allowed, the contractor should be required to ensure that any subcontracting arrangement requires the subcontractor to comply with the privacy provisions of the contract between the contractor and the federal institution. The government institution may also wish to consider, on a case-by-case basis, where appropriate, whether the contractor must receive the institution’s written approval of subcontract provisions before the subcontract is signed.

Step 5.0: Evaluation criteria and sample RFP and contractual language

The comprehensive assessment of federal contracts, initiated by the Treasury Board of Canada Secretariat, revealed that most of the contracts identified by institutions as having potential privacy risks involved data processing and management. To assist such institutions, the following examples of RFP clauses relate specifically to database development, location, and data processing and are intended to be ***applied only in circumstances*** where the privacy risk is assessed at a very high level.

Definition: A database is an organized collection of data that can be accessed quickly. Databases consist of fields, records, and tables. A field is a single piece of information (e.g. a telephone number); a record is a collection of fields (e.g. name, age, telephone number); and a table is a collection of records. To access information from a database, a database management system (DBMS) is needed. A DBMS is a collection of programs that enables the user to enter, organize, and select data in the database.

Database creation is the establishment of the structure of the database but not its data content. One must first create a database, then populate the database and, finally, process the data that is in the database.

Important note: In situations where the personal information is considered to be of a highly sensitive nature, the following sample clauses may be used, where appropriate, to address the risk of potential disclosure to foreign governments. Use of these clauses should be limited to situations where, in consultation with legal services and privacy officials, and based on the invasion of privacy test, it is determined that there is a high level of privacy risk (e.g. health information, income or financial information). Before implementing the clauses indicated below, institutions must consult their legal services and privacy officials. Government officials must also consult legal services before modifying or adapting such clauses to suit specific needs of a given contract or with respect to other program delivery instruments. Where institutions are subject to the requirements of the GSP, the departmental security officer can provide advice on security procedures required by the GSP.

The sample clauses identified below would need to appear in both the RFP and the contractual agreement.

Sample clauses for an RFP and contractual agreement

Canada has an obligation to ensure that Canadian statutes, regulations, and policies on privacy protection are respected. Where applicable, federal institutions must ensure that personal information is protected in accordance with the *Privacy Act*, R.S. 1985, c. P-21, the *Personal Information Protection and Electronic Documents Act*, 2000, c. 5, and federal privacy policies. Therefore, for the purposes of this requirement, where personal information will be involved in the contract, Canada requests the following from the Contractor:

Database and data processing

Where international trade obligations **do not** apply:	Where international trade obligations **do** apply:
Database creation	
1. The database must be located and only accessible in Canada.	1. The database must be located and only accessible in jurisdictions the laws of which do not override, conflict with, or impede the application of the *Privacy Act*, R.S. 1985, c. P-21, the *Personal Information Protection and Electronic Documents Act*, 2000, c. 5, and Treasury Board privacy policies either expressly or through subsequent application.
2. The database must be physically independent from all other databases, directly or indirectly, that are located outside Canada.	2. The database must be physically independent from all other databases, directly or indirectly, that are located in jurisdictions whose laws override, conflict with, or impede the application of the *Privacy Act*, R.S. 1985, c. P-21, the *Personal Information Protection and Electronic Documents Act*, 2000, c. 5, and Treasury Board privacy policies either expressly or through subsequent application.
Data processing	
1. All aspects of data processing must be conducted and only accessible in Canada.	1. All aspects of data processing must be conducted and only accessible in jurisdictions whose laws do not override, conflict with, or impede the application of the *Privacy Act*, R.S. 1985, c. P-21, the *Personal Information Protection and Electronic Documents Act*, 2000, c. 5, and Treasury Board privacy policies either expressly or through subsequent application.

Certification from the Bidder stating the following:

The Bidder hereby certifies that it has reviewed the requirements of this RFP, the resulting contract clauses and, in particular, the requirements concerning the protection of personal information. The Bidder also certifies that it will comply with those terms and ensure that personal information that is managed, accessed, collected, used, disclosed, retained, received, created, or disposed of in order to fulfil the requirements of the Contract shall be treated in accordance with the *Privacy Act* R.S. 1985, c. P-21, the *Personal Information Protection and Electronic Documents Act*, 2000, c. 5, and Treasury Board privacy policies.

This certification shall be true and correct throughout the term of the resulting contract with the same force and effect as if continuously made throughout the term of the resulting contract.

Furthermore, the Bidder acknowledges that the Minister shall rely on this certification to award the contract. Should the Bidder fail to comply with this certification or in the event that verification or inspection by the Minister discloses a misrepresentation on the part of the Bidder, the Minister shall have the right to treat any contract resulting from this bid as being in default and to terminate it pursuant to the default provisions of the contract.

Note: It may be appropriate for government institutions, in certain circumstances where the privacy risk is determined to be high, to make the Contractor's access to the personal information conditional upon the certification remaining true. This way, as soon as a contractor is presented with an order that compels the production of personal information, the certification would no longer be valid and any subsequent access or disclosure of the personal information would constitute a breach of the contract and, in some cases, a breach of Canadian law related to security of information and privacy.

Contacts for more information

Questions regarding the application of the Treasury Board policy on *Privacy and Data Protection* and the *Contracting Policy* should be directed to the appropriate responsibility centre within institutions.

Should you have any questions related to the guidance provided in this document, please do not hesitate to contact the Information, Privacy, and Security Policy Division, Procurement and Project Management Policy Directorate, Treasury Board of Canada Secretariat, at (613) 941-7176.

References

Policy on Privacy and Data Protection
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/siglist_e.asp

Privacy Impact Assessment Policy
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp

Contracting Policy
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/Contracting/contractingpol_e.asp

Government Security Policy
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

Risk Management Policy
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/riskmanagpol_e.asp

Integrated Risk Management Framework
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

Standard Acquisition Clauses and Conditions (SACC) Manual
http://sacc.pwgsc.gc.ca/sacc/contents-e.jsp

Industrial Security Manual
http://www.ciisd.gc.ca/text/ISM/ch1-e.asp

Appendix A: Invasion-of-privacy Test

An invasion-of-privacy test provides guidance in determining whether a contract that would involve personal information would result in harm or injury to an individual. There are three main factors that should be taken into account in any invasion-of-privacy test: sensitivity of the information, expectations of the individuals, and probability and gravity of injury.

1) Sensitivity of the information

Determine what type of personal information will be involved in the contract.

- How detailed is the personal information (tombstone data such as name and address or highly detailed personal information, including longitudinal information)?
- What is the severity of the breach (determined by such factors as the number of individuals whose information is in the database and the amount of individual information collected)?
- Is the information of a highly sensitive personal nature (e.g. health and financial information) or does it appear to be fairly innocuous information (e.g. tombstone information)?
- What is the purpose of the work (i.e. statistical in nature, program administration, regulatory enforcement, or possible criminal enforcement)?
- What is the context surrounding this information? (The name and address of an individual can be innocuous or extremely sensitive depending on the context; for example, names and addresses of individuals participating in a youth employment program are less sensitive than a similar list containing names and addresses of Hepatitis C and HIV compensation victims.)
- What is the amount of control that the service provider will have over the information?

From a privacy standpoint, particular attention should be given to the decision related to contracting highly sensitive information. If information is highly detailed, sensitive, and extremely personal, institutions should consider alternatives that increase the institutions' direct control over the information where possible. Alternatively, institutions should consider implementing a very high standard of security and confidentiality that may be well beyond the minimum requirements when contracting the handling of such information. This will assist in providing Canadians with a comfort level when it comes to their personal information.

Note: The invasion-of-privacy test suggested above has been adapted from the public interest invasion-of-privacy test outlined in paragraph 6.13 of Chapter 2-4 of the Treasury Board policy on *Privacy and Data Protection*.

2) Expectations of the individual

Determine or establish the expectations of the individuals with respect to their personal information. **The conditions that govern the collection of the personal information usually are the best source for determining the expectations of the individuals.**

- Where personal information has already been collected by the government institution, verify what conditions were established at the time the information was first collected from the individual:
- Was there a commitment or promise not to disclose to any other party or institution?
- Was there a caveat stating that the information could be disclosed in a manner consistent with the original purpose for its collection?
- Was the information compiled or obtained under guarantees that preclude some or all types of disclosure?
- Was the information unsolicited or given freely or voluntarily with little expectation of it being maintained in total confidence?

If personal information is to be collected by the government institution from the contractor, or the government institution has exercised control over the contractors' records, establish the conditions for the collection and the expected use and disclosure of the personal information in accordance with the fair information practices embodied in the *Privacy Act* and its regulations as well as the Treasury Board policy on *Privacy and Data Protection*. For example:

- Will the institution provide clear direction to the contractor regarding its obligation with respect to the collection of personal information on behalf of the Government of Canada?
- Will the institution ensure that the contractor informs individuals of the purpose of the collection and obtains consent (where relevant) for the collection, use, and disclosure? This also includes ensuring that individuals are informed of any statutory authority for the collection, of their right to refuse to provide any or all of the requested information and any possible consequences of such refusal, and of their right of access and correction.
- Will the institution ensure that the contractor informs individuals of other possible uses and disclosures related to the information?
- Would an individual feel comfortable knowing that his or her personal information could be accessed by a third party under contract?
- Would the individual expect a third party to be involved in the handling of such personal information?
- What level of confidentiality and security would the individual expect?

3) Probability and gravity of injury

Determine the probability of injury if the personal information was wrongfully disclosed or if a breach of security or confidentiality occurred. Injury should be interpreted as any harm or embarrassment that will have direct negative effects, for example, on an individual's career, reputation, financial position, safety, health, or well-being. The following factors will assist in determining the extent of probable injury:

- Would the contract involve the personal information of few or numerous individuals (e.g. will the contract deal with one or two individuals or will it involve the personal information of hundreds or thousands of individuals)?
- If the information is considered sensitive, can it be surmised that any disclosure carries a probability of causing measurable injury (e.g. identity theft, fraud, emotional distress, or negative effects on an individual's career, reputation, financial position, safety, health, or well-being)?
- Is there a risk in terms of the possible application of foreign laws (i.e. potential for disclosure to foreign government for uses unrelated to the contract)?
- How grave or serious could the potential injury be?

The following table will assist in determining risks related to possible application of foreign laws as a result of a contract involving the handling of personal information.

No Risk	Databases maintained and processed on a Government of Canada site only, or databases located or maintained off-site and processing conducted by a Canadian company that operates in Canada only. Records storage/archival and disposal handled on a Government of Canada site only or by a Canadian company operating in Canada only.
Low Risk	Databases located or maintained off-site and processed by a company in Canada, with potential access by a foreign subcontractor or potential access by foreign parent company or affiliate (with risk mitigation strategies in place). Records storage/archival and disposal handled off-site by a company in Canada, with potential access by a foreign subcontractor or potential access by foreign parent company or affiliate (with risk mitigation strategies in place).
Medium Risk	Database maintained and processing conducted by a foreign-based company in a foreign jurisdiction (with risk mitigation strategies in place).
High Risk	Database maintained and processing conducted by a foreign-based company in a foreign jurisdiction (with no risk mitigation strategies in place). Records storage/archival and disposal handled by foreign-based company in foreign jurisdiction.

Note: Institutions may wish to consider other factors unique to their situations. For this reason, institutions are encouraged to develop guidelines on the application of the invasion-of-privacy test within their institution.

The use of **effective mitigation strategies** by federal institutions will result in reducing the level of risk. These strategies could include the use of non-technological solutions, such as including the privacy clauses suggested in this document, or the implementation of technological solutions, such as encryption.

Appendix B: Privacy Protection Checklist

The purpose of the Privacy Protection Checklist is to ensure that privacy requirements are taken into consideration during the preliminary planning and implementation stages of the government contracting process.

Notes: In this checklist

"personal information" means information about an identifiable individual that is recorded in any form as established under section 3 of the *Privacy Act*; and

"record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine readable record, and any other documentary material, regardless of physical form or characteristics, and any copy thereof, in accordance with section 3 of the *Access to Information Act.*

YES	NO	N/A	DESCRIPTION
			Control and accountability Determine whether the contractual agreement should specify the following: 1. The types of records or personal information (list them) affected by the contract will remain: a) under the control of the government and subject to the *Privacy Act* and the *Access to Information Act*; or b) the sole property of the contractor;
			2. the contractor shall designate a senior individual within its organization to be the point of contract for complying with privacy/security obligations;
			3. the contractor shall provide the government with an up-to date list of all employees, subcontractors, or agents engaged in the contract who will have access to the personal information;
			4. all employees, contractors of the subcontractors, or agents to whom personal information may be accessible in the performance of the contract shall sign a privacy and confidentiality agreement;
			5. the contractor shall be fully and solely responsible for the actions of its employees, subcontractors, and agents who act on its behalf in the performance of their functions under the contract; and
			6. the contractor shall advise the government in advance in the event of any change in ownership of all or a part of the contractor's business.
			7. the contractor shall immediately notify the government in the event of any proceedings for bankruptcy or insolvency brought by or against the contractor under applicable bankruptcy or insolvency laws or any notice of creditor's remedies.

YES	NO	N/A	DESCRIPTION
			Transborder data flows Determine whether the contractual agreement should specify the following: 8. the limitations on where the records and the personal information (including back-up tapes and archives) may be processed, stored or maintained by the contractor (refer to the accompanying guidance document for advice and for sample clauses); or
			9. that the contractor is prohibited from disclosing and/or transferring any personal information outside the boundaries of Canada, or allowing parties outside Canada to have access to it, without the prior written approval of the government.
			Collection of personal information Determine whether the contractual agreement should specify that: 10. the collection of personal information shall be limited to that which is necessary for the contractor to comply with the contract or the exercise of the contractor's rights, under the agreement;
			11. the contractor must, unless otherwise directed in writing, collect personal information directly from the individual to whom the information relates;
			12. the contractor, at the time of collection of personal information, must notify an individual from whom it collects personal information: ▸ of the purpose for collecting it;
			▸ of any statutory authority for the collection;
			▸ whether response is voluntary or required by law;
			▸ of any possible consequences of refusing to respond;
			▸ of the individual's right of access to and correction of the information; and
			▸ of the number of personal information banks in which the personal information will be retained; and
			13. the contractor's employees must effectively identify themselves to the individuals from whom they are collecting personal information and provide individuals with a means to verify that they are actually working on behalf of the government and authorized to collect the information.
			Accuracy of personal information 14. Determine whether the contractual agreement should specify that the contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the contractor or the government in a decision-making process that will directly affect the individual to whom the information relates.
			Use of personal information 15. Determine whether the contractual agreement should specify that, unless otherwise directed in writing, the contractor shall use the personal information only for the purpose of fulfilling its obligations under the contract.

YES	NO	N/A	DESCRIPTION
			Disclosure of personal information Determine whether the contractual agreement specify the following: 16. the contractor shall be prohibited from disclosing or transferring any personal information, except as necessary for the purposes of fulfilling its obligations under the agreement or unless otherwise directed to do so in writing; and
			17. if the contractor receives any request for disclosure of personal information for a purpose not authorized under the contract, or if it becomes aware that disclosure may be required by law, the contractor shall immediately notify the government about the request or demand for disclosure and must not disclose the information unless otherwise directed to do so in writing.
			Requests for information Determine whether the contractual agreement specify the following: 18. individuals can use an informal process to access records or their personal information directly from the contractor; and
			19. the responsibilities of both the government and the contractor in dealing with requests made under the *Access to Information Act* and the *Privacy Act* with respect to those records or personal information are to be considered under the control of the government but maintained by the contractor.
			Correction of personal information 20. Determine whether the contractual agreement should specify the responsibilities of both the government and the contractor with respect to requests made by individuals under the *Privacy Act* to correct or annotate personal information maintained by the contractor.
			Retention of records or personal information Determine whether the contractual agreement specify the following: 21. the retention and disposal requirements for records or personal information, including the maximum retention period and the disposal methods to be used; and
			22. the conditions governing the disposition of any transitory records that are created or generated by the contractor.
			Protection of personal information 23. Determine whether the contractual agreement shall oblige the contractor to ensure that the personal information is protected against such risks as loss or theft, as well as unauthorized access, disclosure, transfer, copying, use, modification, or disposal.
			Complaints and investigations Determine whether the contractual agreement should specify the following: 24. that the government and the contractor shall immediately notify each other when complaints are received pursuant to the *Access to Information Act* and the *Privacy Act* or other relevant legislation and of the outcome of such complaints; or
			25. the right of the Information Commissioner and Privacy Commissioner to access any records or personal information for the purposes of investigations under the *Access to Information Act* or the *Privacy Act*.

YES	NO	N/A	DESCRIPTION
			Audit and inspection of records or personal information Determine whether the contractual agreement should specify the following: 26. that the government may, at any time and upon reasonable notice to the contractor, enter the contractor's premises to inspect, audit, or require a third party to audit the contractor's compliance with the privacy, security, and information management requirements under the contract and that the contractor must co-operate with any such audit or inspection; and
			27. the requirement of the contractor to maintain specific information to enable the conduct of information audits, i.e. the maintenance of some form of audit trail (electronic or paper form).
			Notification of breach Determine whether the contractual agreement should specify the following: 28. the contractor shall be obliged to notify the government immediately when it anticipates or becomes aware of an occurrence of breach of privacy or of the security requirements of the contract; and
			29. the contractor shall be required to indemnify the government for any liability in connection with any breach of its obligations under the contract.
			Subcontracting Determine whether the contractual agreement should specify the following: 30. the contractor must not subcontract the performance of any part of the services or functions under the contract without prior written approval; and
			31. despite any written approval to subcontract, the contractor remains fully responsible for the performance of services under the contract or subcontract.
			Termination or expiry of the contract Determine whether the contractual agreement should specify the folllowing: 32. all personal information and records must be returned to the contracting authority upon completion of the contract; and
			33. the obligations of the contractor to protect personal information shall continue even after the completion of the contract.

Appendix C: Key International Trade Agreements

Agreement on Internal Trade

The *Agreement on Internal Trade* (AIT) applies to most federal government departments and seven Crown corporations. The AIT applies to the procurement of goods valued at $25,000 or more and to the procurement of services and construction valued at $100,000 or more. The AIT does not apply to procurement related to cultural industries, Aboriginal culture, or national security.

North American Free Trade Agreement

The *North American Free Trade Agreement* (NAFTA) applies to most federal government departments and 10 Crown corporations. NAFTA applies to the procurement of goods valued at more than $38,000 (Canada-U.S.) and $89,000 (Canada-Mexico), to the procurement of services valued at $89,000 or more, and to construction contracts worth $11.5 million or more. For Crown corporations, NAFTA applies to the purchases of goods and services valued at $445,000 or more and construction contracts valued at $14.2 million or more.

The *Agreement on Government Procurement of the World Trade Organization*

The *Agreement on Government Procurement of the World Trade Organization* (WTO-AGP) applies to most federal government departments. The WTO-AGP applies to the procurement of goods or services valued at $261,300 or more and construction requirements valued at $10.0 million or more. The WTO-AGP is a multilateral agreement that aims to secure greater international competition for government procurement.

NAFTA and WTO-AGP

Excluded goods and services for Canada

The following five groups of service contracts are completely excluded from NAFTA and WTO-AGP:

- research and development;
- health and social services;
- financial and related services;
- utilities; and
- communications, photographic, mapping, printing, and publication services.

All procurements can be subject to a determination, on a case-by-case basis and by appropriate levels of authority, of what is necessary for the protection of essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes. If such a determination is made, then the procurement may be exempted from the coverage of the trade agreements.

The following exceptions apply:

- purchases for commercial resale or use in the production of goods for commercial resale;
- for Canada, purchases under set-asides for small and minority businesses; and
- purchases for Transport Canada and Fisheries and Oceans Canada and communications equipment relating to Federal Supply Classifications 36, 70, 74.

Note: Dollar limits shown are known to change with inflation and for other reasons. Notification of such changes are issued through the Contracting Policy Notices.

Source: The above information has been reproduced from the Public Works and Government Services Canada document entitled Bidding Opportunities Under Trade Agreements on the Canada/Nova Scotia Business Service Centre Web site.