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

Guidance on Preparing Information Sharing Agreements Involving Personal Information

Published: 2023-08-22

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-76/2023E-PDF
ISBN: 978-0-660-67711-8

This document is available on the Government of Canada website at www.canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Document d’orientation pour aider à préparer des Ententes d’échange de renseignements personnels

Guidance on Preparing Information Sharing Agreements Involving Personal Information

On this page

Template: Information sharing arrangement between federal institutions
(DOC (Word Document), 82 KB (Kilobyte))

Template: Annexes
(DOC (Word Document), 79 KB (Kilobyte))

Introduction and background

This guidance is designed to assist parties in completing the Information Sharing Agreement (ISA) template as well as its supporting annexes when sharing personal information among federal institutions. All ISAs are unique, and the template and content should be adapted to suit your needs.

This guidance should be considered in conjunction with all applicable federal laws, regulations, policies and guidelines. A detailed assessment may be required to identify privacy risks before being able to implement an ISA. Parties are strongly encouraged to consult their institution’s ATIP Coordinator, privacy advisors, legal advisors, information management advisors and security experts to identify, review and consider all applicable laws and policies that may have an impact on privacy and security issues prior to entering into an ISA.

For this guidance, unless specifically mentioned otherwise, ISAs should be understood as non-legally binding arrangements between two or more federal institutions.

Definitions: Personal information and Information Sharing Arrangement

What is personal information?

Personal information is defined by section 3 of the *Privacy Act* as information about an identifiable individual that is recorded in any form. Examples include:

- contact information; information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual
- information relating to the education or the medical, criminal or employment history of the individual
- any information that can be linked to the identification of an individual, such as an account number, licence number, an Internet Protocol (IP) address, a biometric identifier, or a photographic image

Certain information is excluded from the definition of personal information. For example, information that relates to the position or functions of an employee of a government institution is not considered personal information.

When considering whether information is considered personal, keep in mind that a person's name is not always the determining factor. The definition of personal information includes any recorded information that permits or leads to the possible identification of an individual whether alone or when combined with information from sources that are otherwise available, including public sources. "Possible identification" means a serious possibility. It should be something more than a frivolous chance, but less than a balance of probabilities.

For the purposes of this guidance, the term personal information is to be interpreted broadly and includes “data” when it is relates to an identifiable individual.

What is an Information Sharing Arrangement (ISA)?

The *Privacy Act* does not contain any reference to ISAs. That being said, the basic requirements relating to ISAs can be found in the Directive on Privacy Practices under section 4.2.23 through section 4.2.27.

Information sharing may mean that one party is disclosing information while the other party is collecting information, or that information is exchanged, where both parties are disclosing and collecting information.

The benefits of using an ISA to share personal information among federal institutions include:

- clarifying the obligations and accountabilities of the parties involved
- ensuring compliance with the *Privacy Act* and its related policies
- establishing protocols for addressing security incidents including privacy breaches
- providing awareness and instructions for staff
- ensuring transparency for affected individuals

Deciding whether an ISA is the appropriate tool

Is the information to be shared personal?

Have you reviewed the information to be shared to determine whether it involves personal information as defined under section 3 of the *Privacy Act*?

- ☐ Yes
- ☐ No

For more details on this subject, see
Definition of "personal information"

If the information is not personal information, please see Alternatives to Sharing Personal Information with Other Institutions below

Have you verified your legal authority?

- ☐ Yes
- ☐ No

If your institution seeks to receive personal information, have you verified that your institution has the legal authority (legislation, regulation, or order-in-council) to collect personal information?

It is recommended that you consult with your legal services to ensure legal authority prior to collecting and sharing any personal information.

If you do not have legal authority to collect or share personal information, you may not proceed with any personal information sharing activity.

Do you need an ISA?

- ☐ Yes
- ☐ No

Developing an ISA is recommended when sharing any personal information. If sharing the personal information is required under federal law, then the institution must share in accordance with the requirements of that law. In this case, an ISA is recommended but not strictly required.

Alternatives to sharing personal information with other institutions

Given the privacy implications of sharing personal information, parties should consider whether alternative approaches would be more appropriate.

Where possible, personal information must be collected directly from the individuals concerned instead of by way of an ISA.

Alternatively, using and sharing de-identified personal information should be considered. De-identified information is personal information that has been modified so that the risk of re-identifying the individual is greatly diminished and cannot be readily done.

Where this is used, there should remain little-to-no possibility of re-linking any of the information to identifiable individuals or making undue inferences about groups of individuals.

It is recommended to seek advice from statistical experts when de-identifying information. Such consultations would provide assurance that the information to be disclosed would not result in the re-identification of individuals. You may also contact your institution's privacy experts to assist with determining the level of de-identification required given your proposed information sharing. Further guidance on de-identification, especially when working with small populations, can be found in the Privacy Implementation Notice 2023-01: De-Identification and in the Privacy Implementation Notice 2020-03: Protecting privacy when releasing information about a small number of individuals.

When drafting the ISA, make sure that:

- consideration was given to sharing de-identified information instead of personal information
- when de-identified is to be used, clauses prohibiting the receiving party from re-identifying individuals and prohibiting the onward sharing of that de-identified information are included in the ISA

If personal information is not required, you may consider other types of agreements, such as a memorandum of understanding, a master agreement, or a service level agreement, as outlined in the Guideline on Service Agreements: Essential Elements.

Sharing information available within your institution

In some cases, legislation other than the *Privacy Act* explicitly permits uses or disclosures, within or outside the institution. For example, the *Income Tax Act*, the *Statistics Act*, the *Security of Canada Information Disclosure Act*, and the *Department of Employment and Social Development Act* contain specific authorities for the use or disclosure of personal information.

The program area that has control of the personal information to be shared can determine whether sharing is appropriate with the advice of the institution's privacy and legal advisors. There may be other alternatives, but the benefits and privacy risks associated with a particular option should be assessed before making a decision.

Defining the scope of the ISA

All parties to an ISA must consider what is directly related to the activity to ensure that only the minimal amount of personal information is disclosed and collected. The ISA must include a list of all the personal information

elements that will be exchanged along with the purpose for each and specific restrictions that may apply to any of the elements (such as, the parties may wish to specify that more sensitive personal information elements require stronger protections or impose more stringent conditions on subsequent use or disclosure, for example, if the social insurance number is shared).

Disclosing too much personal information or collecting more personal information than is necessary to fulfill a particular purpose is contrary to the *Privacy Act* and may lead to a privacy breach.

Assessing the risks

In addition to ensuring that they have the legal authority to carry out their information-sharing initiatives, parties must ensure that any related privacy and security risks are addressed before entering into any arrangements to share personal information.

Assessing privacy and security risks can be done in a consistent manner through the use the recommended tools such as a privacy impact assessment (PIA), privacy protocol, or a security assessment and authorization (SA&A), previously known as a threat and risk assessment (TRA), detailed below.

Privacy impact assessment (PIA)

The Directive on PIA outlines a process that provides decision makers with:

- an assessment of the initiative's compliance with the *Privacy Act* and its related policies
- probable impacts associated with issues or non-compliance
- mitigation strategies and timelines to reduce or eliminate privacy risks

Privacy protocols

Under the Policy on Privacy Protection, privacy protocols are a set of documented procedures that are consistent with the principles of the *Privacy Act* for using personal information for non-administrative purposes such as research, statistics, audit, evaluation and policy analysis.

Security assessment and authorization (SA&A)

When sharing personal information, the parties must maintain effective administrative, technical and physical safeguards to protect the information. An SA&A is a process by which federal institutions ensure that appropriate safeguards are implemented in their physical and technological environments. When warranted, all parties involved in the information sharing initiative could be required to conduct this assessment process to evaluate the potential threats and risks to the information as a pre-condition of sharing or require confirmation that such safeguards are implemented and periodically reviewed to ensure protection of the information.

Documenting the decision:

Under section 4.3.2.10 of the Policy on Service and Digital, deputy heads are required to document decisions and decision-making processes. When entering into an ISA, it is recommended that parties summarize the due diligence that led the authorized officials of the institutions to conclude that an ISA is necessary. Appropriate documentation may include a memo to the program head, supporting legal analysis, a PIA or a SA&A.

Drafting the ISA and completing the ISA

template

An ISA should set out the terms and conditions that will govern the sharing of personal information between the parties. An ISA template and annexes for federal institutions is provided as part of this guidance. The ISA should be specific and precise, written in plain language to ensure that all terms are fully understood, provide some flexibility to allow for limited amendments, and be drafted with guidance from program and project officials, privacy policy and information management experts, legal advisors and functional specialists, such as information technology system specialists and security experts.

While this guidance pertains to exchanges of personal information between federal institutions, exchanges of personal information with public institutions in other jurisdictions should include similar sections to the ISA template but reflect the applicable laws of the respective jurisdictions.

A summary of the ISA must be made available to the public as outlined in section 4.2.26 of the Directive on Privacy Practices. For greater transparency, institutions can consider disclosing the full ISA through the Open Government portal or on the institution's website. For more information on using the Open Government portal, please contact the open government team at open-ouvert@tbs-sct.gc.ca.

ISA components

▼ In this section

5. Use
6. Disclosure
7. Access rights
8. Method of exchange and frequency of sharing
9. Information management
10. Security management
11. Addressing suspected security incidents and privacy breaches
12. Retention period and disposition
13. Compliance monitoring and audits
14. Transparency
15. Notice
16. Financial arrangement
17. Review
18. Amendments
19. Termination
20. Conflict resolution
21. Designated officials

The following sections provide further guidance to support parties using the provided ISA template and annexes. Institutions using their own template can still benefit from the guidance, but the terminology and structure may not be exactly as seen here.

1. Preamble

The preamble section of the ISA should outline the reasons for the arrangement, explain why information is being shared instead of being collected directly from the individual(s), describe the potential outcomes that the arrangement seeks to achieve, and provide relevant background information.

Federal institutions requesting to receive personal information should be able to clearly identify the purpose for which the information is needed. The information may be needed for an administrative purpose where it will be used in a decision-making process that will affect the individuals involved, such as for:

- **Authentication and verification**: where personal information is used to compare and confirm the identity of individuals prior to granting access to programs and services, physical areas or information
- **Eligibility to a program or a service**: where personal information is used for determining or verifying eligibility for programs, administering program payments or overpayments, or issuing or denying permits/licences
- **Compliance/regulatory activities**: where the information is used for detecting possible abuses of programs, services or harassment where the consequences are administrative in nature (such as, fine, discontinuation of benefits, audit of personal files or claims)
- **Criminal investigations and enforcement/national security**: where the information is used for purposes related to investigations and enforcement in a criminal context or associated with national security or anti-terrorism activities

2. Provisions

For clarity and to ease an institution's ability to track an ISA, it is recommended that ISAs provide details as to the type and duration of the arrangement.

There are different types of ISAs:

- **One-way disclosure:** One institution discloses personal information to a single institution, without receiving information itself

- **Two-way disclosure:** Two institutions party to the ISA receive and disclose personal information to each other
- **Multi-party, one-way disclosure:** An institution discloses personal information to two or more other institutions, without receiving information itself
- **Multi-party two-way disclosure:** More than two institutions are involved in the collection, use and disclosure of personal information between each other

There are different durations for ISAs:

- **One-time disclosure:** Institutions share personal information on a single occasion. In such a case, information can be provided only once, and the ISA should clearly indicate an entry into force date and an expiry date.
- **Determinate period disclosure:** Information may be disclosed routinely throughout a determined period of time. The ISA must clearly define an entry into force date and an expiry date. Where the defined period exceeds five years, a review clause should be added to ensure that the ISA is reviewed on a periodic basis to be determined between the parties.
- **Unspecified period disclosure:** Personal information may be disclosed routinely throughout an unspecified period of time. The ISA should include an entry into force date and a clause on periodic review.

3. Legal authority for collection and disclosure

Collection

Section 4 of the *Privacy Act* prohibits federal institutions from collecting personal information unless it is directly related to a program or activity of the government institution.

The *Privacy Act* is not the single source of law that sets out rules for federal institutions regarding the collection, use and disclosure of personal information.

Other acts of Parliament contain statutory provisions that specifically authorize, prohibit or regulate the sharing of personal information. For example, the *Statistics Act* authorizes Statistics Canada to enter into agreements with provincial statistical agencies, federal, provincial or municipal government institutions or other corporations.

When first considering sharing personal information, parties must satisfy themselves that it is lawful. This means that all institutions involved in the proposed sharing must ensure that they have their own statutory authority to carry out the proposed information sharing (collecting and/or disclosing) activities.

Notification

With confirmed legal authority, institutions are required to notify individuals of a collection of personal information. As outlined in subsection 5(2) of the *Privacy Act*, parties shall notify the program participants at the point of collection about the need to share their personal information as a condition of program enrolment. Notifications must include the elements described in the Directive on Privacy Practices. For example, under many benefit programs, it may be necessary that personal information be shared between institutions to determine the eligibility to program benefits.

When drafting the ISA, make sure that:

- individuals are notified of the new collection/disclosure at the point of collection, if possible

- a privacy notice has been agreed upon by all parties to the ISA and meets policy requirements

Note: Privacy notices should inform the individual why the information is being collected, of any statutory authority for the collection, how it will be used, and who it will be shared with and why.

Disclosure

Section 8 of the *Privacy Act* states that personal information under the control of a government institution cannot be disclosed without the consent of the individual to whom the information relates, unless the disclosure is permitted in any of the 13 circumstances under subsection 8(2). All subsection 8(2) disclosure provisions are discretionary and any disclosure of personal information pursuant to this section must be considered on a case-by-case basis.

In certain cases, the sections of the *Privacy Act* that authorize disclosure do not specify who must make the decision. Although there is no rule about who that should be, it is important that an appropriate official be identified as having made the decision to authorize the disclosure for the purposes of accountability and transparency.

The sharing of personal information could, in some situations, implicate the *Canadian Charter of Rights and Freedoms* (the Charter). The fact that a disclosure is specifically authorized under other acts of Parliament does not automatically ensure compliance with the Charter. It is recognized that the interrelationship between these areas of law is quite complex and legal advice will be necessary.

When drafting section 3 of the ISA, make sure that:

- your ISA collects only personal information that is “directly related to a program or an activity of your institution”

- you have consulted your legal services to establish the collection authority
    - Consent (described below) is not sufficient authority to collect personal information
- you have consulted the TBS Privacy Policy suite, including Directive on Social Insurance Number if you intend to collect or disclose the SIN
- you have determined whether the arrangement qualifies for a disclosure provision under subsection 8(2)
- You have verified whether your own institution's legislation is further restricting the disclosure of personal information than subsection 8(2) of the *Privacy Act*

4. Accuracy of personal information and compliance with standards

Accuracy

Parties to an ISA should base administrative decisions on current and up-to-date personal information. This is especially important where the impact of an administrative decision on individuals might be high. Providing unreliable, inaccurate or incomplete information to other institutions can create potentially serious problems for those who rely on the information, as well as those who are the subjects of the inaccuracies.

When drafting, make sure the ISA:

- contains an obligation to notify the other party if the institution become aware of inaccurate personal information that has been shared
- requires the other party to review any administrative actions taken based on inaccurate information provided

- includes a process to treat any requests for correction made by the individual

Applicable standards

Institutions must make every reasonable effort to ensure that all personal information disclosed – which includes all associated metadata used to describe it – is relevant and meets applicable standards (such as for quality). This is particularly important when personal information will be used in a decision-making process that affects individuals. Prior to sharing the information, parties must clearly establish the type, extent and quality of the personal information and associated metadata to be shared, as well as the method of transmitting it. Steps required to ensure that the personal information is appropriate for the intended use may need to be addressed by the parties before entering into any arrangement to share it.

One example of the importance of personal information that complies with standards is when it includes criminal intelligence. In those cases, the disclosing federal institution could indicate the reliability of the information involved by providing background information – including if it was observed, heard from a source or obtained by electronic intercept, and its origin. In this example, the ISA would have to include caveats to address any concerns about the quality of the personal information or metadata describing it.

Paragraph 4.3 of the ISA template includes provisions with regards to the standards that the institution is following to ensure that the personal information is of high quality.

When drafting the ISA, make sure that:

- the format of the personal information, including its associated metadata, is specified in the ISA so that it is “readable” by the other

party. The exchanged information and metadata should be inter-operable between the parties and standardized in accordance with the Policy on Service and Digital and the Standard on Metadata
- personal information received from external parties, governmental or otherwise, has been profiled and validated prior to its use or reuse. This practice involves complying with any applicable enterprise-level standards needed to enable their structural and semantic interoperability
- information exchanges will be adequately recorded or logged on the subject's file by the disclosing institution, when reasonable, in case of a need to correct inaccurate information

5. Use

Section 7 of the *Privacy Act* prohibits the use of personal information by a federal government institution without the consent of the individual to whom it relates, except for the purpose for which it was collected or for a use consistent with that purpose.

Secondary use

Any prohibitions on secondary uses should be agreed to prior to entering into any arrangement to share personal information. Where appropriate, procedures to seek approval for additional use should be articulated in the ISA, taking into consideration relevant laws, regulations, or policies applicable to each party to the ISA.

When drafting, make sure the ISA:

- identifies how the personal information to be shared under the ISA will be used
- describes any planned secondary uses and is updated when new secondary uses are identified

- specifies that secondary uses are limited to those that are in accordance with section 7 of the *Privacy Act*
- describes any limitations against subsequent or secondary use of the information, taking into consideration relevant laws, regulations, or policies applicable to each party to the ISA
- includes clauses defining procedures to seek approval to further use, along with any other appropriate conditions

6. Disclosure

Subsection 8(2) of the *Privacy Act* describes the circumstances under which personal information under the control of a government institution may be disclosed without the consent of the individual to whom the information pertains. Such disclosures are discretionary and are subject to any other act of Parliament.

Of note, paragraph 8(2)(j) of the *Privacy Act* authorizes the head of a government institution to disclose personal information to any person or body for research or statistical purposes, if the head of the government institution who has control of the records:

- is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates and
- obtains from the person or body a written undertaking that the information will not subsequently be disclosed in a form that could reasonably be expected to identify the individual to whom it relates

Secondary disclosure

Any prohibitions on secondary disclosures should be agreed to prior to entering into any arrangement to share personal information. Where appropriate, procedures to seek approval for additional disclosure should

be articulated in the ISA, taking into consideration relevant laws, regulations, or policies applicable to each party to the ISA.

When drafting, make sure the ISA:

- identifies how the personal information to be shared under the ISA will be disclosed
- describes any planned secondary disclosures and is updated when new secondary disclosures are identified

When determining whether a potential disclosure is aligned with subsection 8(2) of the *Privacy Act*, it is recommended that institutions engage privacy and legal experts.

7. Access rights

ISAs are subject to access to information and personal information requests. As such, the ISA should include clauses about the process that will be used to answer such requests, whether parties want to be consulted, how the consultation process ought to be conducted and which party should be responsible for addressing the request.

When drafting the ISA, make sure that:

- it contains clauses to establish a consultation procedure to respond to *Access to Information Act* or *Privacy Act* requests
- it includes clauses requiring the parties to inform with each other when they receive an access to information request and intend on disclosing information

8. Method of exchange and frequency of sharing

Defining the method and frequency for sharing information is important to ensure that the collection and disclosure of the personal information occurs as anticipated by both parties and is in line with legal and policy requirements. In addition, defining the method and frequency of exchange will better prepare institutions to react quickly should information be accessed or handled improperly.

Information can either be “pushed” (instigated by the disclosing party) or “pulled” (instigated by the receiving party). Regardless of the method, institutions should transfer the relevant information to the other party only in the manner, times and dates provided for in the ISA, rather than giving ongoing access to the database in which personal information is stored.

When drafting, make sure the ISA:

- establishes the process and the frequency by which personal information will be exchanged between the parties has been agreed upon by the parties. Consult Annex D – Transmission and safeguarding of information for examples of how this could be articulated
- includes alternative processes and technologies for sharing in case the primary process or technology is temporarily unavailable

9. Information management

The information collected, used, disclosed or disposed of must be managed in accordance with legislation, the Policy on Service and Digital, the Policy on Privacy Protection and their supporting policy instruments. This is further outlined in Annex D – Transmission and safeguarding of information.

The Directive on Service and Digital requires institutions to use digital systems as the preferred means for managing information. Leveraging enterprise systems where possible can increase the efficiency of information exchange.

Government institutions must have their information management practices and controls defined, documented, implemented, assessed, monitored and maintained throughout all stages of the information life cycle to provide reasonable assurance that information is adequately protected in a manner that respects legal and other obligations, and balances the risk of injury and threats with the cost of applying safeguards.

Parties should take steps to ensure that their information management practices are aligned with those with whom personal information is being or will be shared. The Government of Canada Enterprise Architecture Framework sets out enterprise architecture requirements to ensure that information management practices are aligned across the government.

When drafting the ISA, consider these best practices:

- Use digital systems to create, collect, manage, use and share personal information
- Clearly define roles, responsibilities and accountabilities for personal information in the federal institution via departmental governance structure, both at the working and senior levels
- Ensure, when required, that personal information datasets are updated at appropriate intervals
- Regularly assess the value and utility of personal information assets to ensure that collection and use of personal information is limited to what is required for a program or activity

10. Security management

Appropriate security controls are essential to support the trusted delivery of programs and services. In the context of personal information sharing, it is essential that measures are in place to enable the secure transfer and storage of personal information.

In accordance with the Policy on Government Security and section 4.5.1 of the Directive on Security Management, federal government employees are responsible for adhering to government security policy and departmental security practices, including safeguarding information and assets under their control, whether working on-site or off-site.

The ISA should include clauses to explain that the information shared amongst the parties is treated in accordance with the security designation of the information and on a "needs to know" basis so that only authorized employees have access to the relevant information at the appropriate time.

Any security measures that are appropriate to ensure the security of the personal information during and after transmission, such as encryption, password protection, or authentication should be fully documented in the ISA. Tagging or watermarking the information shared, especially when it is sensitive information, is one way of ensuring that the information will be treated in a manner that respects the terms and conditions of the ISA.

The nature of the safeguards used to protect personal information from both external and internal risks will vary depending on the sensitivity of the information that has been collected; the amount, distribution and format of the information; the method of storage; and the harm or injury that would arise from a breach of security. More sensitive information will be safeguarded by a higher level of protection. To this end, government institutions as defined under section 11.1 of the *Financial Administration Act* should follow the requirements of the Policy on Government Security the

Policy on Service and Digital, and other associated standards and directives. Institutions that are not subject to the FAA should refer to their own internal security policies and procedures.

Moreover, the safeguards should take into account actions to be taken to respond to security incidents or privacy breaches, including the notification of affected parties. For more information, consult Appendix B of the Directive on Privacy Practices.

Often these measures are included in a separate schedule attached to the ISA to allow for flexible amendment whenever the measures are changed. Annex D – Transmission and safeguarding of information, and Annex E – Attestation of consideration of security requirements, provide sample text.

When drafting the ISA, consider:

- whether personal information should be headed or watermarked "Received in confidence pursuant to (title of the ISA)." This could also assist in identifying the source of any unauthorized dissemination
- how institutions entering into an ISA ensure that the personal information being exchanged receives the same security classification on either side (see Appendix J of the Directive on Security Management for more details. Appendix F of that Directive contains a series of security requirements for institutions entering into arrangements that should be respected by federal institutions in the core public service)
- whether the ISA will exchange personal information with institutions who are not subject to the Directive on Security Management, such as Crowns corporations, and whether additional details should be included in the ISAs so obligations are well understood by all parties

11. Addressing suspected security incidents and privacy breaches

Effective reporting and management of security incidents and privacy breaches are essential to ensuring that each Party to the ISA is compliant with privacy and security requirements. The ISA template and Annex G – Protocol for suspected security incidents including privacy breaches requires the notification of all parties to the ISA of any suspected privacy breach. The Preliminary Reporting Tool can be used for the purpose of this notification.

Many privacy breaches are security incidents. Therefore, it is essential that privacy officials in each institution coordinate their response with security officials. Similarly, all security incidents involving information assets should be brought to the attention of privacy officials, who are best placed to determine whether information is personal in nature.

Additional policy requirements include establishing procedures for notifying individuals affected by privacy breaches. Documenting in the ISA which institution will notify individuals in what circumstances could help streamline the breach management process.

More details on managing security incidents can be found in the Directive on Security Management and its Appendix G: Mandatory Procedures for Security Event Management Control, and further guidance on managing privacy breaches can be found in Annex B of the Directive on Privacy Practices.

When drafting the ISA, make sure that:

- the ISA includes breach requirements in the event of accidental or unauthorized access, disclosure, use, modification and deletion of personal information (see ISA template Annex G – Protocol for suspected security incidents including privacy breaches)

- the ISA requires each Party to follow their institution's plans in the event of a breach. It is further recommended that, once a material breach has been determined, institutions use the Office of the Privacy Commissioner's *Privacy Act* Breach Report form for reporting to TBS and the Office of the Privacy Commissioner (OPC)
- both privacy and security officials have been included in the contact information provided in the ISA
- a clause about coordination between institutional privacy and security officials has been included in the ISA

12. Retention period and disposition

Retention of personal information

The *Library and Archives Canada Act* outlines broad legislative direction as it relates to the retention of government records. Additionally, the *Privacy Act* and its Regulations require that personal information used by a government institution for an administrative purpose be retained by that government institution for at least two years following the last administrative use of the information, unless the individual consents to its earlier disposition.

Under the Directive on Service and Digital, each government institution is responsible for establishing, implementing and maintaining retention periods for information resources of business value. It is incumbent upon each government institution to understand and apply any legislation regarding the retention and disclosure of information and, more specifically, its own legislation when setting those retention periods.

The parties to an ISA should indicate a retention period for the personal information shared under the ISA. Parties should ensure that the retention period is no less than the two years provided under section 7 of the Privacy

Regulations.

Disposition of personal information

The disposition of personal information is similarly governed by the *Privacy Act* and the *Library and Archives of Canada Act*. However, the requirements of disposal are less prescriptive and are left to policy instruments to define. For this reason, consulting with your institution's information management experts is recommended.

Information exchanged in the course of an ISA that is subject to a litigation hold must **not** be disposed of before the end of the litigation or the end of all appeal possibilities. Institutions should consult with their legal services if they find themselves in such a situation.

The ISA should explain how the parties plan to dispose of the personal information.

Depending on the sensitivity of the personal information shared, institutions may require to be notified when destruction has taken place. This would require a record of destruction or a log of the disposition of any shared personal information.

Such record of destruction or log could contain the following information and be made available to the other party immediately upon its request:

- details of the records that were disposed of (such as, file name, file number, date(s) of the records)
- the method of destruction (paper copy shredded or electronic copy deleted from all files)
- the date of destruction (day, month, year)
- the name and position title of the person who carried out the destruction of the records

The parties to an ISA may also want to use ISA Annex F – Certificate of destruction of personal information and data elements to attest to that the personal information and data in their possession was destroyed and disposed of.

When drafting, make sure the ISA includes:

- a retention period of the personal information and, if required, clauses for obtaining consent from individuals for early disposal
- an indication of whether the personal information is expected to be returned to the institution or destroyed by the receiving institution at the conclusion of the ISA
- whether a record of destruction will be used by the institutions party to the ISA
- a process for identifying and communicating any litigation holds, personal information requests or access to information requests that would prevent the destruction of any personal information for all party to the ISA

13. Compliance monitoring and audits

Audits help ensure that parties to an ISA adhere to the terms and conditions of the arrangement. Audit provisions also help to strengthen security and privacy controls by encouraging parties to ensure that their information and privacy controls are as effective as possible to meet all their compliance requirements.

When drafting the ISA, determine:

- whether the parties want to use management audits to evaluate their respective information management practices and to assess their compliance with the requirements of the ISA

- whether the parties agree to provide a copy of their respective management audit reports and any action plans to each other within a prescribed time of their completion
- whether clauses in the ISA should request specific audits according to a pre-determined schedule

14. Transparency

Section 4.2.27 of the Directive on Privacy Practices requires that, where possible by security requirements, parties entering into an ISA publish a summary containing the following details, as outlined in Annex K – Summary of the Arrangement to be published:

- title
- name of the program
- identity of the federal institutions who are party to the ISA
- date of entry into force
- date of termination and/or review (depending on the type/length of ISA)
- purpose (including the reason for, type and length of the ISA)
- legal authorities
- personal information being disclosed and collected (including the personal information bank title and number)

The *Privacy Act* also requires personal information under the control of the institution to be described in a personal information bank (PIB). When collecting personal information through an ISA, institutions must engage with their privacy experts to identify the relevant PIB and validate whether it requires any changes or updates resulting from the ISA.

When drafting the ISA, determine:

- what are the security requirements and any other confidentiality or legal considerations when making the ISA or a summary of the ISA publicly available. In most cases, a summary of the ISA should be possible, even if some details need to be withheld
- what is the parties' preferred platform for public disclosure. In addition to the requirements under the Directive on Privacy Practices to publish annual updates in Info Source, parties should also consider using existing platforms such as the Government of Canada's Open Government portal for public disclosures. In the event that institutions consider the Open Government portal, they are encouraged to contact the open government team at open-ouvert@tbs-sct.gc.ca and to comply with TBS policies and directives on information management and communications, such as the Policy on Service and Digital and the Directive on Open Government.
- whether you have consulted your privacy experts to determine whether an update to a PIB is needed

15. Notice

Parties to an ISA should provide each other, as soon as practicable, notice of any change in legislation, regulation, policy, technology or funding relating to their respective programs that may impact their ability to fulfill their obligations as described in the Arrangement.

All notices should be made in writing by the designated officials who signed the ISA or their delegate as outlined in Annex H of the ISA template and should be clear and concise with the objective of communicating specific changes affecting the ISA and potentially the ability to meet obligations.

When drafting notices, institutions should consider including the following details:

- Which clause(s) of the ISA are impacted
- A clear description of the events leading to the change
- Details of whether the change is likely to cause delay
- Details of when the change is expected to take effect
- What mitigation measures have been or will need to be taken
- In cases where institutions are using cost recovery, details of whether the cost recovery amount is likely to be affected

16. Financial arrangement

Some institutions may want to include cost-recovery provisions in their ISAs with other institutions. Paragraph 16 of the ISA template and Annex J provides more details on examples of these types of clauses.

Parties should familiarize themselves with financial policy requirements and confirm they have the appropriate authorities to initiate cost recovery. The Directive on Charging and Special Financial Authorities and the FAA should help parties in determining their authorities for cost recovery, in consultation with their institution's legal services.

Other considerations include determining whether the arrangement is a multi-year arrangement where the costs would carry on throughout the life of the arrangement, or if the arrangement is for a specific fiscal year where the revenues can only be re-spent during the fiscal year for which the costs were incurred.

A process and timing for the cost recovery will need to be agreed upon by the parties to the ISA.

Example 1: The [Disclosing Institution] will send invoices three times per year. The first invoice will be sent in August to cover information provided in April and July, and the second invoice will be sent in mid-February (to ensure payment by March 31) to cover information provided in October and

January. If required, the [Disclosing Institution] will reconcile costs with the actual expenditures to date and, if necessary, proceed with an adjustment for the variance.

Example 2: The [Disclosing Institution] will send an invoice in September of each year, following the annual provision of information, scheduled for August 15 of each year. The [Receiving Institution] agrees to reimburse the [Disclosing Institution] for these costs. If required, the [Disclosing Institution] will reconcile costs with the actual expenditures to date and, if necessary, proceed with an adjustment for the variance.

17. Review

In cases where the duration of an ISA exceeds a period of five years, parties to an ISA should include a clause to ensure that the ISA is reviewed on a periodic basis to be determined between the parties. See paragraph 17 – Review of the ISA template for an example of such clause. More frequent reviews can be considered where needed.

18. Amendments

Amendments to the terms of an ISA or the related annexes should be made in writing and executed by the designated officials or their authorized representatives. Refer to paragraph 18 of the ISA template for suggested wording. Parties to the ISA should include clauses in the ISA defining the amendment process to the ISA or its annexes.

In instances where an amendment changes the collection, use, disclosure to third parties, transfer between parties, disposal or other aspects of the management of the personal information, the institutions must change

their related PIBs. If the changes are substantial, the institutions must also provide TBS with the updated PIB as well as a privacy impact assessment, as outlined in section 4.1.7 of Directive on Privacy Practices.

Should amendments to the terms of an arrangement result in new consistent uses or new disclosures, the institutions must modify their PIBs accordingly and notify the OPC of the new consistent uses, as outlined in section 4.1.17 of the Directive on Privacy Practices.

Coming into force

An ISA comes into force on the effective date agreed upon by the parties and continues to be in force unless it is terminated in accordance with the procedure set out in paragraph 19 of the template or it is replaced by another agreement.

19. Termination

The termination of an ISA or of an annex should be done in writing, either following mutual consent of both parties, or by one of the parties providing a termination notice to the other. Notice must be provided to the institution's designated official for the arrangement. Despite the termination of the ISA, the conditions associated with the sharing of the personal information and the related clauses normally continue to apply to the information that has already been exchanged. Parties to the ISA should include clauses defining how the information should be disposed of at the conclusion of the ISA. Where cost recovery provisions are included in an ISA, the obligation for account reconciliation and the issuance of a final invoice, when appropriate and subject to the termination of the arrangement would also continue.

Upon termination of an ISA, the parties should advise their ATIP offices and update their related PIBs.

When drafting the ISA, make sure that:

- the ISA has a clause to ensure that it is reviewed on a pre-determined, periodic basis (review of ISAs at least every five years from their signature date or more frequently is highly encouraged)
- the ISA includes provisions to allow the parties to terminate the ISA immediately and may request the return of personal information that has been shared
- the ISA contains clauses where amendments to the ISA and the annexes are made in writing and executed by the signatories of each institution or their representatives in the form of an official letter
- the ISA contains amendment process clauses and termination clauses.

20. Conflict resolution

In the event of questions, challenges or disagreements related to any issue connected to an ISA, it is recommended that clauses be included to provide a mechanism for conflict resolution. Paragraph 21 of the ISA template provides sample text.

In cases where conflicts are unable to be resolved, the head of the institution or the Deputy Minister (when applicable) would typically be the ultimate level of conflict resolution.

When drafting the ISA, determine:

- whether the ISA needs to contain conflict resolution clauses to address interpretation questions and challenges, or disagreement associated with the ISA

21. Designated officials

An ISA should include the date, names, titles and signatures of the designated official of all parties involved in the ISA. You may want to refer to paragraph 21 of the ISA template and relevant sections of annexes A, B and H for sample language.

The level of the delegation to sign ISAs depends on the sensitivity of information, the magnitude of any cost recovery involved, and the powers conferred through legislation. Arrangements deemed to be low risk or low cost are often signed at the director or the director general level.

When the personal information is more sensitive or when the costs are higher, either the head of the institution or a deputy minister or assistant deputy minister equivalent may wish to sign.

Broad ISAs that act as overarching arrangements comprised of smaller annexed arrangements are often signed by heads of institutions or deputy ministers (when applicable). The signature of amendments to annexes in umbrella ISAs could be delegated to an authorized representative who would be responsible for the program area. This allows for greater flexibility should the content of those annexes need to be amended.

Typically, the signing authority for the respective parties to the ISAs is equivalent but this may differ if a specific authority is identified in legislation. For example, if the deputy minister is signing the ISA for Party A, the respective deputy minister or equivalent should be the signatory for Party B. This practice extends to interjurisdictional ISAs whereby the provincial or territorial signing authority would be at the same level as their federal counterpart.

Definitions

The definitions of the terms “administrative purpose,” “head of institution,” “personal information,” and “personal information bank” shown below are consistent with the manner in which these four terms are defined in section 3 of the *Privacy Act*. The other definitions have been adapted for the specific use of this guidance document.

administrative purpose (fins administratives)
is the use of personal information about an individual “in a decision-making process that directly affects that individual” (section 3). This includes most uses of personal information for confirming identity (authentication and verification purposes) and for determining eligibility of individuals for government programs

aggregated data (données agrégées)
describes data in statistics that is combined from several measurements, or in economics, describes high-level data that is composed of a multitude or combination of other more individual data. In all cases, “aggregated data” should have been generalized in such a way that it cannot be linked to an individual, for example, by using a range of ages rather than specific ages

authorized representative (représentant autorisé)
is a representative authorized by the designated official for carrying out specific terms and conditions of the arrangement and who can amend the annexes of the ISA, except for a new use of personal information

consent (consentement)
is the informed, voluntary agreement of an individual for the indirect collection or for the disclosure, retention and subsequent uses of personal information collected from the individual for a legally authorized purpose

consistent use (usage compatible)
is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This

means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out

data (données)

is the set of values of subjects with respect to qualitative or quantitative variables representing facts, statistics or items of information in a formalized manner suitable for communication, reinterpretation or processing

de-identification (dépersonnalisation)

is personal information that has been modified through a process to remove identifiers to a degree that is appropriate in the circumstances. De-identified information carries a residual risk of re-identification

designated official (fonctionnaire désigné)

is the person designated by a federal institution as the signatory to an ISA that will have the overall administrative responsibility for the ISA and its related annexes

head (responsable d'institution fédérale)

is the minister, in the case of a department or ministry of state. In any other case, it is the person designated by the *Privacy Act* Heads of Government Institutions Designation Order. If no such person is designated, the chief executive officer of the government institution, whatever their title, is the head

non-administrative purpose (fins non administratives)

is the use of personal information for a purpose that is not related to any decision-making process that directly affects the individual. This includes the use of personal information for research, statistical, audit and evaluation purposes

notice (avis)

is the indication given to another institution about possible changes to an ISA

privacy notice (avis de confidentialité)
is a verbal or written notice informing an individual of the purpose of a collection of personal information and of the government institution's authority for collecting, including creating, using and disclosing the information. The notice, which must reference the PIB described in Info Source, also informs the individual of their right to access, and request the correction of, the personal information and of the consequences of refusing to provide the information requested

program or activity (programme ou activité)
is, for the purposes of the appropriate collection, use or disclosure of personal information by government institutions subject to this policy, a program or activity that is authorized or approved by Parliament. Parliamentary authority is usually contained in an act of Parliament or subsequent regulations. Parliamentary authority can also be in the form of approval of expenditures proposed in the Estimates and as authorized by an appropriation act. Also included in this definition are any activities conducted as part of the administration of the program

personal Information (renseignements personnels)
is "information about an identifiable individual that is recorded in any form." See section 3 of the *Privacy Act* for additional information

personal information bank (PIB) (fichiers de renseignements personnels)
is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the PIB has been used, is being used, or is available for use for an administrative purpose and is under the control of a government institution

social insurance number (SIN) (numéro d'assurance sociale (NAS))
is a number suitable for use as a file number or account number or for data-processing purposes, as defined in subsection 28.1(3) of the *Department of Employment and Social Development Act*. For purposes of

paragraph 3(c) of the *Privacy Act*, the SIN is an identifying number and is therefore considered to be personal information

sensitive personal information (renseignements personnels sensibles) while virtually any personal information may be sensitive in certain contexts (for example, disclosure of a home address may expose an individual to risk for personal or professional reasons), there are certain categories of personal information that are considered sensitive for all or most individuals. These include medical, financial information, criminal history, or widely used personal identifiers such as the SIN or other information, the disclosure of which could be injurious to the individual to whom it relates (such as, identity theft, fraud, emotional distress or negative effects on an individual's career, reputation, financial position, safety, health or well-being)

Reference documents and useful links

Federal legislation and useful links

- *Access to Information Act*
- *Canadian Charter of Rights and Freedoms*
- *Library and Archives of Canada Act*
- *Privacy Act*
- *Privacy Regulations*

Policies, directives and guidance

- Directive on Open Government
- *Directive on Privacy Impact Assessment*
- *Directive on Privacy Practices*
- *Directive on the Social Insurance Number*
- *Directive on Departmental Security Management*
- Guide to Integrated Risk Management

- *Policy on Access to Information*
- *Policy on Privacy Protection*
- *Policy on Service and Digital*

Date modified:
2023-08-03