



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Canada

The Digital Privacy Playbook

Published: 2023-03-27

© Her Majesty the Queen in Right of Canada,
represented by the President of the Treasury Board 2023,

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

Catalogue Number: BT48-34/2023E-PDF
ISBN: 978-0-660-48404-4

This document is available on the Government of Canada website, [Canada.ca](https://www.canada.ca)

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Le Guide sur les pratiques relatives à la vie privée numérique



The Digital Privacy Playbook

The Playbook summarizes important and timely privacy advice, all in one place.



You can reference this tool early and often to:

- plan for privacy considerations throughout all stages of your initiative
- incorporate privacy guidance into the development cycle
- identify when and how to contact privacy experts
- understand what privacy deliverables will be required

Key information for each stage of your initiative

Apply privacy protections throughout the life cycle of your initiative.

What stage are you in?



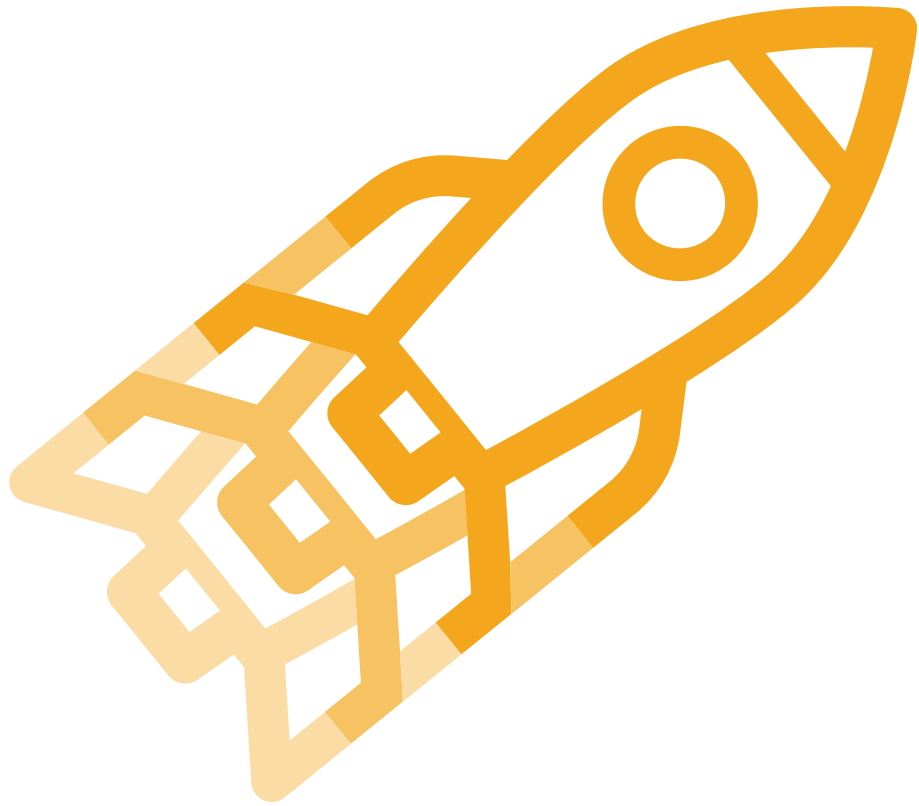
Plan



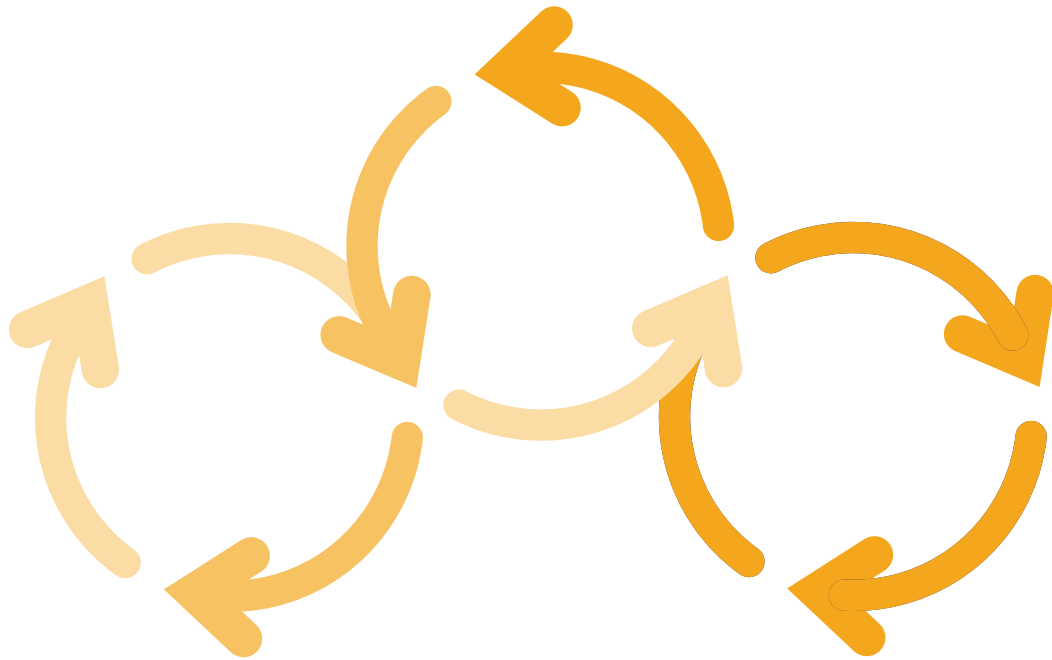
Design



Review



Launch



Update

Not sure what stage you're in? Get a [complete privacy guidance checklist](#).

Key topics in privacy guidance



Planning for privacy

Engage your privacy experts



Identify your personal information



Ensure authority to collect



Handling personal information

What and how to collect



How to use and share



When to keep and delete





Safeguarding personal information

Establish safeguards



Deal with privacy breaches quickly



Common privacy deliverables

Privacy Notices



Privacy Impact Assessments



Personal Information Banks



Information Sharing Arrangements



Guides and templates

[Core Privacy Impact Assessment template](#)

[Information Sharing Arrangement guidance](#)

[Privacy Breach Management Toolkit](#)

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**

Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-31



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Planning for privacy

- Engage your privacy experts
- [Identify your personal information](#)
- [Ensure authority to collect](#)

Engage your privacy experts

Before starting your initiative, find out who your privacy experts are so you can engage them early in your process.

How they can help

Your institution's privacy experts can help you throughout your initiative to:

- determine the privacy requirements you'll need to follow
- avoid or mitigate any potential privacy risks
- find out whether you'll need to complete any privacy deliverables
- understand what's involved in creating these deliverables

Getting in touch

Most institutions have a generic inbox you can use to get in touch with your Access to Information and Privacy office or Privacy Management Division. Otherwise, you can search [this list of access to information and privacy coordinators](#) who'll be able to guide you in the right direction.

Next →

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Planning for privacy

- [Engage your privacy experts](#)
- Identify your personal information
- [Ensure authority to collect](#)

Identify the personal information in your initiative

It's important to have documentation about the personal information involved in your initiative readily available for your privacy experts. This will help them to determine whether your initiative needs a Privacy Impact Assessment or any other privacy deliverables.

Before engaging your privacy expert, put together a list of all the information involved in your initiative, including:

- if it's personal information
- its purpose in connection to your initiative, whether it's a need to have or nice to have

- how it will be used, such as for administrative or non-administrative purpose
- any details you might have on how it will be shared

Make sure it's clear how each piece of personal information plays a critical role in achieving your objectives to ensure you're only collecting the least required.

Identifying personal information

Personal information is any information that can be used to identify an individual, such as their name, home address, email address, telephone number, or date of birth. Even a number or symbol can be considered personal information if it can be attributed to an individual. Identifying personal information could depend on the context, circumstances, or how the information is combined.

Administrative versus non-administrative use

When listing the information involved in your initiative, make sure to include how it will be used, such as for:

Administrative purpose

Information used to make a decision about an individual, such as eligibility for a benefit or confirming someone's identity when logging into an online account

Non-administrative purpose

Information used for research, statistics, or for an evaluation of your initiative

Scenario: Can I make do with less?



Who

Claire, a program manager, wants to collect 6-digit postal codes to offer a benefits program to citizens living in rural communities.

Situation

Because the program targets people in rural communities, her privacy advisor cautions that a 6-digit postal code may indicate the exact address of somebody's home.

Outcome

Claire decides to collect a 3-digit postal code instead because it is sufficient to track the regional participation of her program's applicants, while ensuring it doesn't unnecessarily reveal personal information.

← Previous

Next →

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Planning for privacy

- [Engage your privacy experts](#)
- [Identify your personal information](#)
- Ensure authority to collect

Get authority to collect the personal information

This is a critical first step in ensuring a successful initiative.

Legal authority

You must be legally allowed to collect, create, or use the personal information involved in your initiative. In the privacy world, this is referred to as legal authority. Simply put, you can't collect and/or use personal information without the legal authority to do so, regardless of whether your initiative needs it to meet its objectives.

Privacy tip

Getting consent to collect an individual's personal information doesn't replace having legal authority.

How to confirm legal authority

Legal authority for your initiative can be found in departmental or program-specific legislation.

A [full list of policies, regulations and laws by department or agency](#) may help you identify whether your initiative has legal authority to collect and use personal information.

If you still don't know whether you have legal authority, you should reach out to your institution's legal services unit. They will be able to advise on whether legal authority exists and if not, what is required to obtain it.

[← Previous](#)

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Handling personal information

- [What and how to collect](#)
- [How to use and share](#)
- [When to keep and delete](#)

What and how to collect personal information

What to collect

Once you've determined what personal information is needed for your initiative, you can start collecting it. Make sure you're only collecting:

- personal information that has a direct connection to your initiative
- the least amount required to meet your objectives

Privacy tip

It's important to remember that the more personal information your initiative collects, the greater the impact of a potential privacy breach.

How to collect

Before you collect, make sure an individual has access to read or hear a privacy notice before providing you with their information.

Collecting directly or indirectly

You should aim to collect personal information used for administrative purpose directly from the individual. This ensures that it's as accurate and up to date as possible.

That said, there may be instances when your initiative needs to collect that information indirectly, meaning, from somewhere other than the original source. This is usually the case when, for example, an individual has authorized someone else to provide information on their behalf.

Privacy tip

When collecting personal information indirectly, make sure that it is coming from a reliable source and verify its accuracy before using it.

Getting consent for indirect collection

If your initiative is collecting personal information indirectly, you'll most likely need to get consent. Even if you get consent to collect the personal information, you'll still need legal authority.

When getting consent, make sure it's properly documented, such as in writing. Inform the individual providing you with their consent about:

- the purpose of the consent and the specific personal information involved
- who'll be asked to provide personal information
- the reason why the information is being collected indirectly
- any consequences that may result from withholding consent
- any alternatives to providing consent

Plan in advance for situations where an individual refuses to provide their consent or when you are un-able to get their consent because it will:

- result in collecting inaccurate information
- defeat the purpose of the collection
- bias the use of the information collected

Next →

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Handling personal information

- [What and how to collect](#)
- How to use and share
- [When to keep and delete](#)

Using and sharing personal information

Once you've collected the personal information needed for your initiative, you'll need to ensure it's managed properly throughout its lifecycle.

Using personal information

Your initiative can only use the personal information for:

- the reason it was originally collected, or
- a consistent use: a reason directly connected to the initiative's original purpose

When thinking about using and sharing personal information for non-administrative purposes, such as for research, statistics, auditing and evaluating the program, consider:

- other alternatives, such as the use of aggregate data or de-identified personal information
- whether the benefits of collecting this personal information outweigh the potential invasion of privacy
- how you will establish a ruleset or protocol to properly handle this information

Scenario: Can I evaluate my initiative in a privacy-friendly way?



Who

James, a program manager, wants to determine if his initiative's benefit was effective in reaching equity-seeking groups.

Situation

An evaluator on his team suggests using disaggregated data from the initiative and linking it to de-identified survey data that their institution has access to. They do so and perform an analysis of the data.

Outcome

The evaluation reported that younger, visible minority workers were more likely to have received the benefit than older non-visible minority individuals. They were able to determine these findings in a privacy-friendly way by using disaggregated and de-identified data.

Although evaluating an initiative's effectiveness is a reasonable non-administrative use of information, make sure to engage the experts to ensure proper disaggregation and de-identification of information.

Sharing personal information

If your initiative shares personal information with third parties, including other government institutions, make sure you have an Information Sharing Arrangement (ISA). An ISA will outline the rights, responsibilities and accountability of each party.

Privacy tip

Personal information should not be shared for any purpose other than its original intent or a consistent use unless the individual gives their informed consent.

There are situations where personal information can be shared outside of its original purpose.

Examples of these instances include:

- complying with an Act of Parliament that allows the information to be shared
- complying with a subpoena or warrant issued by a court

- when it is in the public interest (in cases such as an emergency)

A full list of instances when personal information can be shared be found in the [Privacy Act](#).

Even with these exceptions, there may be circumstances where an ISA is needed. Your privacy expert will be able to help you determine when one is needed.

← Previous

Next →

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Handling personal information

- [What and how to collect](#)
- [How to use and share](#)
- [When to keep and delete](#)

When to keep and delete personal information

A retention and disposition plan is a schedule for how long your initiative intends to hold onto personal information and when it will be destroyed. It should include a rationale as to why the personal information needs to be kept, for how long, and how to properly dispose of it when it's time to do so.

When you need a retention and disposition plan

Your initiative always needs a retention and disposition plan for personal information it collects, creates, uses or shares.

How long to keep personal information

Depending on how the personal information is used, there may be legal obligations to hold onto it for a certain time period. For example, personal information used to make a decision about someone must be held onto for at least two years, since the last time it was used. This gives the person time to make a request to access their information.

Your initiative may determine that, to meet its needs, personal information should be kept for longer than two years. Your initiative can delete personal information earlier than two years if it no longer needs it and the individual has agreed to its destruction.

Privacy tip

Your retention and disposition plan will depend on the context and circumstances of your initiative, so long as it can be rationally justified.

When to update and review your retention plan

Your retention and disposition plan should be reviewed and/or updated any time the initiative changes how it collects, creates, uses, or shares personal information. This is to make sure your plan still makes sense and meets all the requirements of the [Privacy Act](#). These modifications to the handling of personal information may also require an update to your initiative's Privacy Impact Assessment and related Personal Information Bank.

← Previous

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Safeguarding personal information

- Establish safeguards
- [Deal with privacy breaches, quickly.](#)

Establish safeguards

Before you launch your initiative, make sure you have a plan to limit access and protect personal information through physical, technical and administrative safeguards.

You should be reviewing and updating your safeguards any time there are physical, technical or administrative changes to your initiative. This could involve new ways of handling personal information, including the use of a new system or platform, or staff turnover.

Physical safeguards

Physical safeguards are ways to protect your institution's physical assets, and include:

- ensuring employees only have access to the floors or rooms where they have security clearance
- registering visitors at the front desk
- locking your screen when you leave your desk
- appropriately storing physical documents or records, according to their classification

Technical safeguards

Technical safeguards are ways to protect electronic data, and include:

- limiting access to systems or software that host personal information as well as establishing role-based access within a system or software
- keeping a log of all the instances where personal information has been accessed, modified, or deleted
- regularly reviewing who has access to personal information and whether that access is still needed
- a means for your initiative to use de-identified or anonymized information to decrease risks involved in sharing personal information

Your institution's IT Security team can help you to establish various technical safeguards to protect your personal information.

Administrative safeguards

Administrative safeguards are policies, procedures and practices that protect privacy. Examples include:

- Information Sharing Arrangements (ISA)
- a privacy protocol
- privacy awareness training

Providing regular and up-to-date training is important so that all employees, third parties and contractors understand their roles and responsibilities in protecting personal information and preventing privacy breaches.

Privacy tip

It's especially important to include safeguards in any contract or ISA when you're working with third parties.

Privacy Training essentials courses:

- [Access to Information and Privacy Fundamentals: COR502](#)
- [Privacy in the Government of Canada: COR504](#)

Next →

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:
2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Safeguarding personal information

- [Establish safeguards](#)
- Deal with privacy breaches, quickly

Deal with privacy breaches, quickly

A privacy breach is the improper or unauthorized collection, creation, use, sharing, retention or disposal of personal information. A privacy breach may occur within an institution or off-site. It may be the result of inadvertent errors or malicious actions by employees, third parties, including partners in information sharing arrangements or bad actors.

Primary causes of a privacy breach

The most common cause of a privacy breach is human error, for example:

- a misdirected email or postal mail containing personal information, such as an email with login credentials or a postal package that includes a passport
- not protecting equipment that contains personal information. For example, transferring a hard drive without clearing its data

- unauthorized access to personal information, such as snooping in a database
- collecting more information than is needed
- holding onto personal information for longer than you needed or for longer than you indicated in your retention plan

Scenario: Why can't I access my old files?



Who

Marie, a program officer, gets a new portfolio of files right before she leaves on vacation for a month.

Situation

When Marie returns, she tries to access her former portfolio and keeps getting denied. After three attempts, she's locked out of her account and must request an official password change with the administrator of the system.

Outcome

Marie is frustrated but realizes that since she got a new portfolio before her vacation this prevented her from accidentally accessing files that are not hers. This shows that the safeguard implemented to limit unauthorized access was successful.

Material privacy breaches

Material privacy breaches involve a real risk of significant harm to an individual. This includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, identity theft, and financial loss.

These types of breaches must be reported to the Office of the Privacy Commissioner of Canada (OPC) and to the Treasury Board of Canada Secretariat (TBS).

Preventing a privacy breach

Ideally, you want to prevent breaches from happening. Implementing safeguards is an important first step, but you're also advised to create a plan for dealing with a privacy breach, before it happens.

Your initiative must have a plan to respond to privacy breaches affecting any personal information under its control. This includes personal information shared with or collected by third parties as part of a contract or agreement.

The plan to respond to a privacy breach must:

- include roles and responsibilities
- align with any security requirements
- meet the privacy policy requirements

Privacy tip

When responding to a breach, be careful not to take any steps that would make the situation worse or lead to another breach, for example sharing additional personal information.

Managing a privacy breach

There are four steps to respond to a breach in privacy:

Step 1: Identify and contain the breach

If your initiative suspects a privacy breach, employees must try to control it right away. Then, employees should notify privacy and security officials of the potential or confirmed breach.

Step 2: Complete a full assessment of the breach

Your initiative needs to work with the privacy experts to decide whether a full assessment of the breach is needed.

Step 3: Mitigate and Communicate the impacts of the breach

When the breach is contained, work with your privacy experts to put in place measures to reduce the risk of it happening again, including informing the public.

Step 4: Prevent another breach

Your initiative needs to put in place prevention measures to reduce the risk of a future breach occurring. These measures must be put in place within a suitable time frame.

At this point, the privacy experts will need to complete a formal report to inform the OPC and TBS if the breach is considered a material breach.

Privacy Breach Management Toolkit

← Previous

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Common privacy deliverables

- Privacy Notices
- [Privacy Impact Assessments](#)
- [Personal Information Banks](#)
- [Information Sharing Arrangements](#)

Privacy Notices

A privacy notice lets people know what you're doing with their personal information.

When you need one

Any time your initiative collects personal information from an individual, you're required to let them know what you're doing with it. Your privacy expert can help you determine whether your initiative needs a privacy notice and review your content. Always make sure an individual has access to read or hear a privacy notice before providing you with their personal information.

Privacy tip

Depending on whether people are providing their personal information online, by mail or over the phone, you may want to adjust the way you present your notice. For example, you would provide a hard copy privacy notice in a paper application, but a call center agent may read a summary of the notice out loud and let the caller know a full notice is available elsewhere.

What's required

Your privacy notice must include:

- why you're collecting an individual's personal information
- your legal authority to collect and use it
- whether the information will be shared with any other parties
- the consequences of not providing information. For example, if the individual doesn't complete an application form with their personal information, then they can't receive the benefit
- the individual's right to access and correct any personal information they provide
- the relevant Personal Information Bank number they can use to exercise that right
- the individual's right to file a complaint with the Office of the Privacy Commissioner if they aren't satisfied with the way their information is handled

General process

- once you've drafted your notice, share it with your privacy expert for their review
- depending on your institution, various approvals may be needed

When to update and review

If there are any changes to the way your initiative collects or uses personal information, you'll need to update your privacy notice accordingly. You may also want to schedule a regular review of the notice to ensure it remains accurate. If there are any changes required to the Privacy Impact Assessment, that's also a great time to update your notice.

Next →

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Common privacy deliverables

- [Privacy Notices](#)
- Privacy Impact Assessments
- [Personal Information Banks](#)
- [Information Sharing Arrangements](#)

Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is a policy process to identify, assess, and mitigate potential privacy risks before they happen.

When you need one

Institutions need to develop and update a PIA anytime:

- an initiative uses or intends to use personal information to make a decision about an individual, or
- there is a substantial change to the way personal information is, or will be, used to make a decision about an individual. This can include your initiative contracting out or transferring any part of the initiative



Privacy tip

Your privacy expert may ask you to answer a few short questions to determine if you need a PIA.

If your initiative doesn't make decisions about an individual, but does collect and/or use personal information, consult your privacy experts to determine if any privacy assessment, such as a privacy protocol, or other deliverables are needed.

Scenario: Do I need to update my PIA?



Who

Samira, a program advisor, is working on a benefits program that's moving their traditionally paper-based application process online.

Situation

The new application portal requires people to create an account in order to submit their application to the initiative. Samira needs to know whether she needs to update any of her privacy deliverables.

Outcome

Her privacy officer explains that since there is a significant change to the way information is being collected, she'll need to update her PIA.

What's required

All PIAs must include:

- the name and brief description of the initiative
- what personal information you're collecting, such as name, phone number, etc.
- your legal authority to collect, use, and share the personal information
- how you're collecting personal information, such as by paper, video, audio, etc.
- a diagram of how personal information will move to deliver the program
- an analysis of how personal information will be handled, who will have access to it and how it will be shared
- where the personal information will be stored, for how long and how it will be deleted
- a completed Risk Area Identification and Categorization (Appendix C-Core PIA)
- a summary analysis of the risk(s) and recommendations for their mitigations

General process

- reach out to your privacy experts
- complete all the required sections of the PIA
- your privacy expert will help determine if you need a Personal Information Bank (PIB)

- your privacy experts can review your PIA, determine any risks in your plan, and help develop mitigation strategies
- if you need a PIB, you should send it for approval with the PIA
- get the PIA approved and signed off, as appropriate within your institution, and send a copy to the Office of the Privacy Commissioner of Canada and the Treasury Board Secretariat
- all these steps need to be completed before the launch of the initiative

When to update and review

Your PIA should be continuously reviewed and updated any time there are changes to your initiative. Always contact your departmental privacy expert to assist you in determining which parts of the PIA need updating.

Related links:

- [Directive on Privacy Impact Assessments](#)
- [Risk Area Identification and Categorization](#)

← Previous

Next →

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Common privacy deliverables

- [Privacy Notices](#)
- [Privacy Impact Assessments](#)
- Personal Information Banks
- [Information Sharing Arrangements](#)

Personal Information Banks

A Personal Information Bank (PIB) is a description of personal information collected and held onto by an institution as it relates to its programs or activities.

When you need one

Your privacy expert can advise on whether your initiative will need to create or update a PIB. Typically, you'll need one if your initiative uses, has used or has available for use personal information for an administrative purpose.

What's required

All PIBs must include the following information and headers:

Description

A brief description of the information collected for the initiative

Class of individuals

Who your initiative will collect information from

Purpose

Why your initiative is collecting this information and under what legal authority it is being collected. Ensure that you cite the same legal authority as noted in the related Privacy Impact Assessment (PIA)

Consistent uses

How information is being used in connection to the initiative's original purpose

Retention and disposal standards

How long will the information be held on to

Records Disposition Authority (RDA) number

A number assigned by Library and Archives Canada

Related record number

A number of a related Class of records, which is a description of information maintained by an institution in support of an initiative, if applicable

Treasury Board of Canada Secretariat (TBS) Registration

A number assigned by TBS, once the PIB is registered

Bank number

A unique PIB number assigned by your institution

Last updated

The date of the last review and update of the PIB

General process

- complete all the required sections of the PIB (your privacy expert can help you with the RDA and bank number)
- get the PIB approved by the delegated head of privacy for your institution
- email the PIB to the Treasury Board of Canada Secretariat's (TBS) [privacy_generic_inbox \(Privacy.vieprivee@tbs-sct.gc.ca\)](mailto:privacy_generic_inbox@tbs-sct.gc.ca) along with the related PIA
- TBS will assign a registration number to the PIB
- once the PIB is registered, your institution's privacy office will make sure it is included in the institution's inventory of information holdings

Privacy tip

A new PIB needs to have a related PIA. So, if you're working on a PIB, then you're likely working on a PIA as well. You can prepare both deliverables at the same time leveraging the existing content from one to the other and submit them together.

When to update and review

You should be continuously reviewing and updating your PIA and PIB any time there are changes to the way your initiative collects/creates, uses, shares, or retains personal information.

← Previous

Next →

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

Common privacy deliverables

- [Privacy Notices](#)
- [Privacy Impact Assessments](#)
- [Personal Information Banks](#)
- Information Sharing Arrangements

Information Sharing Arrangements

An Information Sharing Arrangement (ISA) is a written record of understanding between the parties that will be sharing information. Information sharing may mean that one party is sharing information while the other party is collecting information. It can also refer to a situation where both parties are sharing and collecting information.

When you need one

Your initiative will need an ISA if it shares information with any third party, including other government institutions.

Benefits of an ISA include:

- clarifying the rights, obligations and accountability of the parties
- ensuring compliance with applicable privacy protection legislation and policies
- establishing protocols for addressing problems and incidents (including privacy breaches)
- ensuring transparency for affected individuals

What's required


An ISA should be drafted with advice and guidance from stakeholders in the program area, privacy policy and information management advisors, legal counsel and functional specialists, such as information technology specialists and security experts.

It should include:

- the purpose of the ISA
- what personal information will be collected, created, used and shared between the parties
- the legal authorities to collect, use and share the personal information
- the associated Personal Information Bank(s)
- which institution has custody and control over the personal information
- any limitations on how personal information can be shared between all the parties
- all the administrative, technical and physical safeguards needed to protect personal information
- processes for addressing privacy and security breaches, including notification requirements



Privacy tip



Defining custody and control of personal information in an ISA is very important to make sure it is clear who will be in charge in case of a privacy breach.

General process

- complete all the required sections of your ISA
- send it to your privacy experts so they can make sure it aligns with privacy policy
- socialize the ISA with all the parties and stakeholders involved
- submit the ISA for approval
 - it's up to your institution to decide the appropriate level of approval
 - this can also differ depending on the exact nature of the ISA and level of risk involved

All these steps need to be completed before the launch of the initiative.

When to update and review

When initially drafting an ISA, the parties should agree on when the arrangement comes into force, when and how to review it and when it terminates. The parties may also wish to indicate when and how to change the ISA if there are any changes to technical, legal or other aspects of the initiative.

Related link:

- [Information Sharing Arrangement Guidance](#)

← Previous

Did you find what you were looking for?

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-27



[Canada.ca](#) › [About Government](#) › [Government in a digital age](#)

› [The Digital Privacy Playbook](#)

A privacy guidance checklist

This checklist should help give you a better idea of what privacy guidance you should be following and when, while completing your initiative.



Plan

Depending on your initiative, some of these steps may have already been completed.

- create a list of all the personal information involved in your initiative
- for each piece of personal information on your list, indicate:
 - why you need it
 - how it will be used and shared
 - whether you have legal authority to collect it
- send this information to your privacy expert



Design

Once you know what privacy deliverables are needed, get started right away. Depending on the complexity of your initiative, this work could take a team several months to complete.



review guidance on privacy deliverables to find out what's required for each:

- create a Privacy Impact Assessment (PIA)
- create a Personal Information Bank (PIB)
- create a Privacy Notice
- create an Information Sharing Arrangement (ISA)



ensure personal information will be protected throughout the initiative

- develop access controls and other safeguards
- ensure there's a plan to prevent privacy breaches



create a strategy for how your initiative will hold onto and delete information

- your initiative needs a retention and disposition plan for the personal information it collects, creates, uses, or shares
- information for an administrative purpose should be kept for at least two years since its last use



Provide privacy training to all individuals who will have access to personal information

- The Canada School of Public Service offers Privacy

Training essentials courses:

- Access to Information and Privacy Fundamentals: COR502
- Privacy in the Government of Canada: COR504



Review

These steps may differ from one institution to the next, depending on its structure and available resources.



consult the appropriate stakeholders to review your privacy deliverables

- stakeholders may include experts in privacy, law, information management and information technology specialists, etc.



submit your deliverables for approval at the appropriate levels in your institution

- if you created an Information Sharing Arrangement (ISA), make sure it's been signed by all parties
 - the appropriate level of approval can change depending on the exact nature of the ISA and level of risk involved
- create a schedule to regularly maintain and update your privacy deliverables and processes
- make sure all employees have completed the privacy training you provided



Launch

- publish your privacy notice before collecting any personal information
 - depending on the way your initiative collects information, your privacy notice may be delivered online, as a paper copy, or a call center agent may provide a summary out loud
- continue to address any risks identified in your Privacy Impact Assessment (PIA)



update access controls if there have been any changes in staffing or roles

- your access controls should be updated any time there are any new hires, departures or changes to positions or files



make sure any new staff have completed the privacy training

- consider including privacy training as part of your onboarding for new staff who have access to personal information



Update



continuously review and update your privacy deliverables and processes, especially if there are any changes to the way information is handled

- despite best efforts, a privacy breach can still happen. Make sure to modify your breach plan based on any lessons learned, even after launch

Yes

No

What was wrong?

- I can't **find** the information
- The information is hard to **understand**
- There was an error or something **didn't work**
- Other reason

Please provide more details

You will not receive a reply. Don't include personal information (telephone, email, SIN, financial, medical, or work details).

Maximum 300 characters

Submit

Date modified:

2023-03-31