DENTONS

6th Annual Dentons Data Summit

November 2024

Grow | Protect | Operate | Finance

Privacy Impact Assessments on AI systems and projects: a guide

1. Introduction

This Guide is intended to support private sector organizations in understanding, assessing and reducing privacy risks in relation to the use of AI systems and projects when undertaking Privacy Impact Assessments (PIAs) in Canada.[1] This Guide is not a complete solution nor comprehensive PIA – it is focused on the particular considerations relevant to AI and its processing of personal information. Organisations are encouraged to build on existing PIAs deployed within their organization or sector. For instance, public sector organizations and health information custodians will have different considerations and requirements.

This Guide is solely focused on privacy impacts of AI projects. It does not cover AI governance issues generally, or issues related to the ethical deployment of AI or reducing bias in AI. Separate assessments will be required for these areas and not included here.

This Guide deals only with Canadian privacy laws. Organization may have other concerns or obligations related to the laws of other countries in which they have operations or do business.

2. When to use this guide

- When determining if a PIA is necessary
- When determining the likely scope and scale of a PIA
- When undertaking an AI-related PIA
- When periodically reviewing AI-related privacy risks
- When designing, developing, deploying, procuring, or using systems containing AI components.

What is a PIA?	A PIA is a structured methodology that can help you to identify and minimise privacy risks, and realise privacy improvements, when you are starting a new project or making changes to existing initiatives. A PIA is one way to implement 'privacy by design' in your organisation's practices, and it can help you to build and demonstrate compliance with privacy laws. A PIA should involve an assessment of: positive and adverse privacy impacts including community reaction compliance with privacy laws and other relevant legislation

[1] NOT LEGAL ADVICE. Information made available herein is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based up-on this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read herein. Dentons Canada LLP professionals will be pleased to discuss resolutions to specific legal concerns you may have.

measures to reduce any identified risks to privacy.

What is AI? AI is the ability of a computer system to perform tasks that would normally require human intelligence, such as learning, reasoning, and making decisions. AI encompasses various specialised domains that focus on different tasks and includes automation.

Examples of ways an organization might seek to use AI include:

- an AI-powered chatbot on an organisation's website
- AI software that detects faces and counts the number of people visiting a venue
- a piece of software which uses large amounts of data held by the organisation to predict or determine who is eligible for a discount and/or to calculate the discount they are entitled to
- software that uses student records to predict which students are more likely to be identified in subsequent grades as being "at risk"
- a technology that analyses crowd sentiment in a stadium by using CCTV footage combined with social media data and environmental system data to alert the stadium management to changes in customer sentiment during crowded events

There are also different methods of deploying AI systems and solutions within an organization. Some organizations may internally develop their own customized system; others may use a third party AI systems that is hosted (either internally or externally) and could be off the shelf or modified for the organisation's needs.

3. The PIA process when assessing AI systems and projects

When considering a PIA, you will need to refer to applicable privacy legislation, which includes:

- *Personal Information Protection and Electronic Documents Act,* SC 2000, c 5 ("PIPEDA")
- *Personal Information Protection Act*, SA 2003, c P-6.5 ("AB PIPA")
- *Personal Information Protection Act*, SBC 2003, c 63 ("BC PIPA")
- *Act respecting the protection of personal information in the private sector,* CQLR c P-39.1 ("QC Privacy Act")

The first question to ask when assessing whether a PIA is needed is "Will any personal information be collected, stored, used or disclosed in the project?"[2] This is threshold assessment.

Even where the answer is "no", consider documenting the outcome of your threshold assessment, for recordkeeping and due diligence purposes. This record could include:

- a brief project description
- whether the project involves personal information (and if the answer is no, document what information is being used and why it isn't personal information).
- where personal information is being used, document:
    - a brief description of the personal information such as name, address, date of birth, health information, bank details
    - why this information is needed
    - the relevant authority
    - storage and security of the information
    - access to and amendment of the information
- any known or likely views of any stakeholders about the impact of the project on privacy
- whether a PIA is recommended or not
- details of the person or team responsible for the threshold assessment.

If an AI system or project involves handling personal information, a PIA will likely be *required* by the QC Privacy Act.

---

[2] However, even if no personal information is being handled, you might still decide to conduct a PIA if you wish to show how you are avoiding the use of personal information.

In other Canadian jurisdictions, whether to conduct a PIA is ultimately a risk-based decision that should be made on a case-by-case basis. The cost or size of a project or system is not a reliable indicator of whether a PIA should be conducted, as even low-cost or small-scale projects may have significant privacy impacts.

Canadian privacy laws describe the principles that govern how organizations must handle personal information– see Schedule 1 of PIPEDA, for example. The PIA process helps to identify and manage the privacy risks that may arise from using AI systems and projects that involve personal information.

A PIA is a dynamic tool that should be regularly reviewed and updated throughout the development and implementation of an AI system or project. This is because the privacy risks may change as the AI system or project changes its inputs, outputs and impacts. Laws and regulations are also evolving. Frequent reviews and updates to PIAs on AI systems and projects will help to keep track of and address these changes.

What is personal information	'Personal information' is information about an identifiable individual. Information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information AI systems and projects could involve data that, at first glance, may not appear to be personal information: • De-identified information: De-identified information, such as randomly assigned identifiers that distinguish individuals from each other but do not include attributes such as a name, address or driver licence number. Information of this kind could still be considered personal information if a person's identity can be reasonably ascertained by referring to other data sources – even if the organization doesn't have any specific intention to do such an identification. • Inferred information: Because personal information can include an opinion about an individual, AI-generated inferences about individuals are also considered personal information, even if they are incorrect

Plan the PIA: assign responsibilities and describe the project

The nature and size of your project will determine who undertakes the PIA. You may require expertise in a range of areas, including information privacy and data protection, technology and systems, risk management, law and ethics.

PIAs can be conducted internally, externally, or by a combination of both internal and external persons. A PIA conducted by external assessors may be preferable in instances where you do not have internal expertise, or in situations where community trust in the PIA findings and the project are particularly important.

Where your AI model or system is supplied by a third party, the product or system developer may have undertaken their own PIA, which you could use to inform your analysis (but your analysis should still be independent).

You should set out who is responsible for the PIA, the expertise and inputs required, important milestones, key decision-making points and how consultations will be carried out. You should also outline:

- why the project is being undertaken
- the context or setting in which the project is being undertaken including relevant social, economic and technological considerations
- the project's overall aims and objectives and how these fit with the organisation's broader objectives
- any links with existing programs or projects
- the target market of the project
- what personal information will be collected and how it will be stored, used and disclosed and how security and quality are to be addressed.

Stakeholder consultation

Early engagement with the people with an interest in the project, or who will be affected by the project, is essential. Consultation can continue throughout the project lifecycle, so that the necessary people are consulted at the appropriate time or as the project changes. Stakeholder consultation:

- can identify privacy risks and concerns not previously identified and possible strategies to mitigate these risks
- offers stakeholders the opportunity to discuss risks and concerns with the organisation and to gain a better understanding of, and provide comment on, any proposed mitigation strategies
- can gain the confidence of stakeholders and the public/customers/clients that privacy is being taken seriously and managed effectively.

The range and number of stakeholders to be consulted will depend on the size and complexity of the project, the likely privacy risks and the number of people who could be impacted.

Map information flows

The flow of personal information in a project needs to be mapped, detailing what information will be collected, used and disclosed, as well as how it will be stored and protected. Your mapping should describe:

- who will collect what information, and from whom
- how the information will be collected, and for what purpose
- how the information will be used or processed
- how the information will be stored and kept secure
- the processes for ensuring information quality
- whether the information will be disclosed to another organisation or organisation, to whom and for what purpose
- if the information is to be disclosed to and used by secondary users, how well will those secondary users protect that information and whether they will pass it on to others
- whether personal information will be transferred to another organisation in another jurisdiction
- whether and decisions will be made about the individual
- whether individuals will be able to access and correct their personal information and otherwise exercise their privacy rights
- how long the information will be retained and when and how the information will be disposed of.

Mapping information flows will be particularly important where AI systems are used, given that data can be moved around in multiple ways, making it difficult to maintain records and to control access. In addition, information flows will need to take into account where personal information is created (e.g., through inferences).

Identify privacy risks and possible remedial actions

Once you have mapped information flows, you will need to identify and assess the potential privacy impacts of your project. As a first step, it is important to check your project's processes in relation to handling personal information against the privacy obligations set out in:

- applicable privacy laws
- any applicable privacy codes of practice or sector-specific guidance or directives (e.g., OSFI, advertising and marketing industry organization, etc.)
- other legislation that applies to your organisation relating to the collection and use of personal information (e.g., banking or insurance legislation)

Even if the project appears to be compliant with privacy legislation, there may still be other privacy risks that need to be addressed. Some of the key questions to consider include:

- Will individuals lose control over their personal information?

- How valuable would the information be to unauthorised users? For example, is it information that others would pay money for or try to access by hacking?
- How will privacy breaches be handled?
- Is there a visible, comprehensive and effective complaint handling mechanism?
- How consistent is the project with community values about privacy?
- What auditing and oversight mechanisms are in place, especially if a system fails?
- Does the project collect more information than it needs to?

You will also need to consider specific risks to individuals, such as the potential re-identification of pseudonymised data, identity theft or fraud, reputational damage, loss of confidentiality or financial loss.

These risks may be part of a separate existing PIAs for projects involving personal information.

Based on the nature of your project and your handling of personal information, you should consider the likelihood and severity of the risks you identify.

The next step is to consider what action can be taken to resolve these privacy risks. Some options could be that you:

- decide not to collect certain types of data
- reduce the retention periods for some personal information
- anonymise or pseudonymise data where possible
- take additional security measures (both technical, such as access control mechanisms and encryption, as well as physical, such as limited access to certain areas)
- put clear data sharing arrangements into place
- offer individuals the chance to opt out where appropriate
- train staff to ensure risks are anticipated and managed
- prepare internal guidance and processes to avoid risks.

This is not an exhaustive list: the measures you can take to mitigate privacy risks will depend on your project. Where there are multiple options to address a privacy risk, you will need to evaluate the likely costs, risks and benefits of each option to identify which is the most appropriate.

Formulate and consult on draft recommendations

The above analysis will result in a set of recommendations that include an action plan and timeline. These recommendations should identify how privacy protection measures can be enhanced and how negative privacy impacts or risks can be avoided or reduced. The recommendations could address:

- changes to the project that would achieve a more appropriate balance between the project's goals and the protection of personal information
- privacy management strategies that will reduce or mitigate privacy risks
- the need for further stakeholder consultation
- whether the privacy impacts are so significant that the project needs considerable re-design or even its feasibility examined
- creation of privacy documentation or amendment of existing organisation privacy management plans
- issues beyond project specific matters to overall privacy risk management for the organization (e.g., lack of a retention schedule).

You should discuss the proposed recommendations with affected stakeholders before they are finalised, to ensure their views are incorporated and to secure their commitment to the recommended actions.

Prepare the report

The PIA report needs to set out all the information gathered throughout the PIA process. Key elements include:

- introduction and background information, including the context of the project
- project description
- who was responsible for the PIA and the approach they took and date performed
- a description of the information flows
- results of stakeholder consultation
- outcome of risk assessment and compliance check, including privacy risks that have been identified, options considered to mitigate risk, why particular options or alternatives were rejected or discounted and why a particular course of action has been recommended
- description of privacy risks that cannot be mitigated, the likely response to these risks, and whether they are outweighed by the benefit delivered by the project recommendations.

Be aware that in some cases, the PIA report may contain privileged or confidential information, or that its larger circulation may prejudice security measures to protect personal information. Be aware that a privacy commissioner may ask to see a PIA. Consult with counsel to understand how to draft PIAs in a way that protects privilege and/or reduces risk.

You should consider and adopt a position on the recommendations in the PIA report. At a minimum, you should identify whether you will adopt, partially adopt or not adopt any of the recommendations made. You should provide reasons why you have not adopted recommendations.

Review and update

Seeking external review of a PIA by an independent third party can ensure that the PIA has been carried out properly and that the recommendations have been implemented.

Many projects undergo changes before their completion. If the changes are substantial and result in significant new privacy impacts that were not considered in the original PIA, it may be necessary to undertake a new PIA or update the original one.