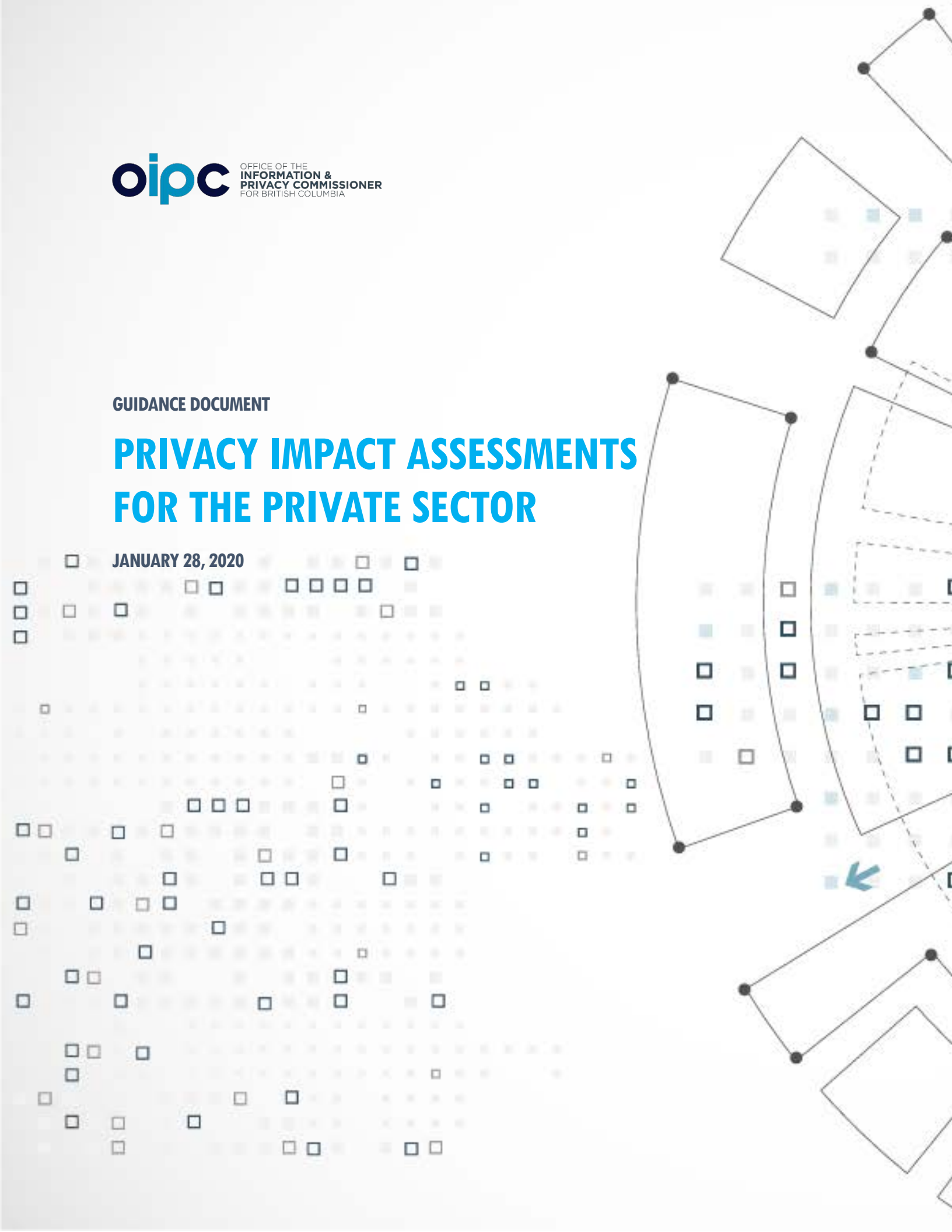
OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

GUIDANCE DOCUMENT

PRIVACY IMPACT ASSESSMENTS FOR THE PRIVATE SECTOR

JANUARY 28, 2020



CONTENTS

PURPOSE OF THIS GUIDANCE DOCUMENT

Private sector organizations in British Columbia are legally obligated to abide by the *Personal Information Protection Act* when it comes to how they collect, use and disclose personal information.

Privacy impact assessments (PIAs) allow organizations to be proactive when it comes to ensuring that the initiatives they have planned comply with PIPA. The Office of the Information and Privacy Commissioner of British Columbia (OIPC)'s Private Sector PIA template aims to assist organizations in making the most of this important tool, both as a tool in the earliest stages of development through to ensuring compliance throughout an initiative's lifespan.

This guidance document provides added depth to the sample language and instruction offered in the template. For more information about PIPA, please refer to our Guide to BC's Personal Information Protection Act for Businesses and Organizations. The structure of this guidance document follows that of the template.

COMMON QUESTIONS

What is personal information?

Under PIPA, "personal information" means information about an identifiable individual that is not contact information or work product information.[1] Previous OIPC orders have interpreted personal information to include information that is reasonably capable of identifying an individual either alone or when combined with information from other available sources.[2] Personal information also includes employee and volunteer personal information.[3]

Some examples of personal information are: name, address, gender, education, income, financial information, medical and genetic information, date of birth, driver's license number, photographs or images of an individual, employment history, biometrics, and product preferences.

[1]Under s. 1 of PIPA, "work product information" is information prepared or collected by an employee as part of that individual's work responsibilities.
[2] Order P12-01, 2012 BCIPC 25 at para. 82.
[3] Under s. 1 of PIPA, "employee personal information" means information collected, used, or disclosed solely for the purposes reasonably required to establish, manage, or terminate an employment relationship between the organization and an individual.

What is a PIA?

A privacy impact assessment (PIA) is an effective tool for assessing new technologies, programs, projects, systems, and activities, hereafter "initiatives," before an organization implements or substantively revises them, ensuring compliance with PIPA.

Why do a PIA?

PIAs help organizations review the intention of the proposed initiatives, identify and prevent expansion beyond the collection's intended purposes, review and accept risks, create policies, and identify positions in the organization that are responsible for handling personal information. They also create documentation that can inform individuals, upon request, about where and when their personal information is collected, used, and disclosed.

Am I legally required to complete a PIA?

While you are not legally obligated to complete a PIA, they add value to your organization by addressing and documenting your legal requirements under PIPA. They demonstrate due diligence and accountability in meeting a commitment to protect privacy and are considered a best practice for all organizations that collect, use, disclose and dispose of personal information.

Who is the audience for my PIA?

The audience for a PIA will depend on your organization. Most organizations write the PIA from a risk mitigation perspective, with the intended audience being the privacy officer, internal staff, and executives. Signing off on a PIA is an acceptance of risk; executives should make sure they understand the contents of a PIA before signing the document.

When should we complete a PIA?

Organizations should complete a PIA whenever there is a new or substantively changed initiative. PIAs are most useful when conducted early in the development of an initiative, as they can be used during the design phase to identify risks and address privacy concerns. Organizations that delay a PIA risk having to make expensive and time-consuming changes to an initiative to ensure its compliance with PIPA.

Do I need to publicly post or share my PIA?

Individuals are only entitled to their own personal information under section 23 of PIPA, with some limited exceptions. However, organizations can publicly disclose their program assessments and sometimes use PIAs for the purpose of transparency.

GETTING STARTED

PIAs involve assessing all aspects of your initiatives from a privacy and, to some extent, security perspective. By examining your initiatives early in their development, you can enhance both privacy and security.

To begin, you will need to gather some key information, including:

- an understanding of your objective/the purpose(s) for collecting, using, disclosing, retaining, and storing personal information;
- the intended scope of the initiative;
- any internal policies about security, retention, and disposal of records; and
- if applicable, any previous PIAs that relate to the initiative.

Other aspects of your proposed initiative may already exist or will develop over the course of completing the PIA. These include:

- how the information will flow through your organization;
- who you intend to have access to the personal information and how this will be controlled;
- whether any of your service providers[4] will assist you in fulfilling your objectives;
- where you intend to store your information, including how it will be secured; and
- how long you intend to retain the information and securely dispose of it once the retention period expires.

PART 1
GENERAL ADMINISTRATIVE DETAILS

The PIA should begin by identifying your organization and, if appropriate, the work unit responsible for the initiative. Understanding where the initiative belongs in an organization will help when updates or changes arise or when seeking information to respond to queries from the public or a regulator.

After you have identified a work unit responsible for the initiative, decide who will draft the PIA. During the drafting process, the author is responsible for document control and creating or collating content. It is advisable that authors work with their privacy office/officer while drafting the PIA. Depending on the initiative, organizations may also need to engage legal, security, program experts, vendors, or other individuals with advanced knowledge of the initiative.

[4] For the purposes of this document, service providers are organizations that collect, use, or disclose personal information from or on behalf of your organization.

After the PIA is approved, the author will be a valuable source of information if there are questions about the document's content. For this reason, it is a good idea to include the name, job title, and contact information of the author of the PIA itself.

PIAs should be living documents. While an approved PIA represents a snapshot of the initiative at the time of signature, organizations should create a review cycle to ensure the initiative is still operating as documented and provide an opportunity for updates over time, as well as to ensure that approving executives have not changed.

1. Initiative description

This section of a PIA should provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, how the initiative fits into any larger processes, how it functions, and the parties involved.

The description of the initiative will be the foundation for the operations and risk analysis section, particularly for understanding how information will flow for the initiative. This information and the scope (outlined in the next section) will assist in creating the notification statement that individuals will receive when providing their consent.

If the initiative will involve other organizations (third parties), this section should explain that role.

2. Scope of the PIA

A PIA should include a statement on the scope of the initiative. This statement should explain, where applicable, exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover. This is an important exercise, as it will assist your organization in understanding the limits of your purpose(s) if there are future initiatives.

Scoping is also useful for large initiatives with multiple possible streams for personal information. Organizations also use scoping to break a larger initiative into multiple PIAs for a narrow analysis of a larger initiative's smaller activities. For example, a new customer management system may have different modules for advertising, assigning tasks and billing. Each of these modules may benefit from their own PIA, or could be included as an addendum under a larger PIA about the overall system.

3. Related documentation

This section should identify other PIAs and documents, such as security assessments or contracts, related to the initiative. This will provide your organization with a central record of how the documents relate to each other and where to find further information.

PART 2
OPERATIONS AND RISK ANALYSIS

4. Collecting personal information

Under PIPA, organizations collect the majority of personal information from individuals through consent,[5] which may be written or verbal. This section documents how organizations intend to obtain consent from the individual through expressed and implicit methods.

If your organization is collecting an individual's personal information without consent, this section explains how you are collecting the information and what section of PIPA authorizes this collection without consent.[6]

If your organization is obtaining personal information from third parties, this section should explain the purposes for and legal basis for the collection.

TYPES OF CONSENT	**Implicit consent**[7] is only valid if a reasonable person would consider the collection, use, and disclosure of personal information by the organization obvious and the individual voluntarily provides the personal information for that purpose.
	Verbal consent is a valid means of collecting consent but it may be difficult for the organization to address concerns from an individual about the collection in the future.
	As a best practice, and where practical, obtain **consent in writing**, rather than verbally. If you are unable to obtain consent in writing, find a way to document where and when the individual provided their verbal consent.

NOTE FROM THE COMMISSIONER	**Consent** is not the only requirement for collection. A reasonable person must also consider the collection of the information appropriate under the circumstances.[8] Organizations must also ensure that they are not requiring an individual to consent to more information than is **necessary** for them to provide the product of service.[9]

[5] PIPA, section 6
[6] PIPA, section 12(2)
[7] PIPA, section 8
[8] PIPA, section 11
[9] PIPA, section 7(2)

5. Implications of withdrawing consent

This section should consider the implications of an individual withdrawing their consent for the collection, use, and disclosure of their personal information. This includes the ability of your organization to offer products and services.[10]

6. Notification statement

When collecting personal information from an individual, organizations are required to disclose to the individual the purpose(s) for collecting their personal information.[11] If requested, your organization must be able to provide the individual with the position name or title and contact information of an officer or employee of your organization who can answer questions about the collection.

This section also builds on information from the 'consent' and 'describing the initiative' sections of the PIA. The privacy officer should be able to read this section and assess what employees will be telling individuals, whether the purpose(s) described are accurate, complete, clear, and concise, and be able to identify the individual responsible for the initiative.

7. Personal information inventory

A personal information inventory is a table containing all of the elements of personal information that the organization collects, uses, discloses, and retains about an individual for the initiative.

The table provides an itemized list of the elements of personal information the work unit intends to collect from individuals directly and indirectly. Even if an individual consents, the personal information must have an appropriate connection to the purpose for collection.[12] A personal information inventory can assist the author of the PIA and the privacy officer in identifying the purpose(s) for each element of personal information and is an easy way to evaluate the need for each piece of personal information.

Completing a personal information inventory can also help to identify the sensitivity of each piece of personal information your organization is seeking to collect. If the author of the PIA is unable to assess the sensitivity of personal information, the privacy officer should fill in this section. If the PIA author fills in the sensitivity section, the privacy officer will want to review it carefully, as the sensitivity of information may change depending on the type and quantity of the other elements of personal information collected.

---

[10] PIPA, section 9
[11] PIPA, section 10
[12] PIPA, section 11

The personal information inventory can identify employees or other users who will need access to the information, which is useful for creating technical and administrative security controls.

Depending on the initiative, your service providers may need access to the personal information in order to assist you with achieving your purpose(s) for the information. You can use the personal information inventory to identify which of your service providers need the personal information to assist you and why.

PIPA requires that you only retain personal information for as long as is necessary to fulfill your business and legal obligations. Noting the retention period in the personal information inventory will assist you in contemplating your business and legal obligations early and in creating policies for retention and destruction. This will also help you create a central document detailing the length of time your organization will retain the personal information.

PIPA gives individuals the right to know the ways in which their personal information is, and has been, used by your organization, as well as the names of individuals and organizations to whom your organization disclosed the personal information.[13] Creating a personal information inventory will allow your organization to quickly and efficiently respond to such requests.

NOTE FROM THE COMMISSIONER	**Limiting collection** is a best practice. Only collect the personal information that you need for your initiative. Collecting too much personal information increases the risk that your organization will have a privacy breach and the severity of any breaches. Over collection of personal information also risks damaging your organization's reputation, as clients may feel deceived or misled through a gradual increase in the use of the individual's information beyond the original intention of the initiative.

8. Personal information data flow table/diagram

Personal information flow tables and diagrams are tools for visualizing your initiative and understanding how personal information moves through your organization.

Flow tables are useful when there is a single direction for information flows, rather than multiple decision points within a decision tree, and to identify the PIPA section authorizing that collection when not relying upon consent. For example, if your organization were operating as a service provider to another private business, you would not have an individual's consent to collect their personal information. However, there are other sections within PIPA that authorize you to collect personal information that was collected with consent by another organization to enable you to assist that organization in fulfilling its purpose.

[13] PIPA, section 23

Your organization can also use flow tables to explain information within the flow diagram. By using a numbering system on the table, you can identify flows and activities within your diagram and use the table to describe the activity and purpose, type of information flow, and PIPA authority for the activity.

Flow diagrams are useful for understanding complex information flows that involve multiple third parties, work units, systems, or decision points. By identifying each point where your organization collects, uses, and discloses personal information, from the client initially providing their information until you have achieved the intended purpose for the information, you can determine whether you are remaining consistent to your purpose(s) and operating with legal authority under PIPA.

PART 3
SECURITY AND UPDATES OF PERSONAL INFORMATION

9. Security measures

Organizations operating in British Columbia have a legal obligation to protect personal information under their custody or control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.[14]

There are three broad types of security measures:

PHYSICAL	These security measures relate to the physical environment that the information is stored in; for example, whether your organization limits access to the filing cabinet or file room through select staff having a key.
TECHNICAL	Technical measures relate to your organization's hardware and software; for example, firewalls, encryption, and intrusion prevention systems.
ADMINISTRATIVE	Administrative controls are rules and processes for your employees or third parties that prevent them from inappropriately accessing, using, or disclosing your client's personal information; for example, role-based access controls, annual privacy training, employee codes of conduct, and privacy-related clauses in contracts.

[14] PIPA Section 34

A PIA should indicate the type, amount, and sensitivity of the personal information, potential risks, and how your organization uses, discloses, and stores the personal information. With these considerations, your PIA should identify what security controls are reasonable and likely to be effective at protecting the personal information.

Template Appendix A – Risk Mitigation Tables

In addition to the PIA, you should conduct a risk mitigation analysis. A risk mitigation table is a helpful tool to assist in this process, allowing you to visualize and document risks to your organization, the probability of them occurring, the potential impact on your organization and affected individuals, and what you intend to do to reduce your risk. An effective risk mitigation table considers how effective your organization's mitigation strategies may be, while recognizing that it is impossible to avoid all risk. This visualization can help your organization's leaders determine whether the risks associated with your initiative are acceptable, as well as to prioritize mitigation strategies and responses to information incidents.

While risk factors can include situations that affect your ability to provide your products and services, the focus should be on your clients. Your risk factors should consider the invasion of an individual's privacy by internal threats, such as employee snooping or lost paperwork, as well as external threats, such as hackers or burglary.

There are five important elements to a risk evaluation.

RISK	Suspected threats to the privacy of your clients
PROBABILITY	A score that identifies the likelihood of the risk occurring.
IMPACT	What could happen to an individual if the risk occurs? The impact score gauges how damaging the impact would be for the individual's privacy.
MITIGATION	Strategies your organization will implement to lessen the impacts and/or reduce the probability of the risk occurring. The mitigation score gauges how effective the mitigation is at reducing the risk.
SCORE	This is an indication of the outstanding risk, after applying the mitigation strategies. This score provides the organization's decision makers with an understanding of the risks the organization will incur if they proceed with the initiative.

Heat mapping, the process of applying colour to risk levels, will provide management with a strong visual of the risks the organization would continue to incur from the initiative. By approving the PIA and initiative, the PIA signatories are indicating that those risks are within the organization's tolerance for risk.

When considering risks involving personal information, remember the volume and sensitivity of personal information collected, used, and disclosed in the personal information inventory. A breach involving a large quantity of personal information with low sensitivity could be just as damaging to individuals and the organization as a breach involving a small amount of highly sensitive information.

Note: in some circumstances, the PIA author and/or privacy officer may need to consult with other members in the organization (IT, programmers, security, marketing) to make sure accurate and complete information is being provided for the PIA risk assessment.

When assessing the probability and impact, consider whether a privacy breach could present a real risk of significant harm to the impacted individuals that the personal information is about. Considering the potential impact of a privacy breach during the PIA stage can help the organization put in place strategies to lessen the risk, and to respond more quickly to such an incident should the risk materialize. For more information on assessing risk in the context of a privacy breach, and when to report a privacy breach to affected individuals and the Office of the Information and Privacy Commissioner, see our guidance document "Privacy Breaches: Tools and Resources."

NOTE FROM THE COMMISSIONER	**Scoring** the probability of risk, impact, and mitigation strategies is not an exact science and relies heavily upon the professional judgement of the assessor. Your privacy officer should understand your organization and be capable of assisting with, or performing, this assessment.

10. Monitoring compliance

Unauthorized access by employees is one of the leading causes of privacy breaches. Understanding who has access to your organization's personal information and why is important for ensuring that your security measures are effective.

An effective audit system should document who accessed personal information and when. As a best practice, systems should aim for "view" audits, as these types of audits are more likely to

find cases of snooping compared to "write" audits, which only trigger an audit trail when an employee changes something about the client's personal information.

You do not need to limit audit capabilities to technical systems. Sign-in sheets can be an effective method of tracking access to locations or physical files when technical audit trails are not appropriate.

When designing systems and processes for monitoring compliance, your organization must also monitor the effectiveness of these controls to ensure they are working effectively. This section of the PIA should outline your plan to evaluate the effectiveness of your compliance controls.

PART 4
ACCESS, ACCURACY, CORRECTION, & RETENTION

11.Individuals requesting access to their own personal information

PIPA gives individuals the right to access their own personal information, the ways that the personal information was used by your organization, and the names of individuals and organizations to whom your organization disclosed the personal information.[15] Your organization must provide individuals with access to their personal information and the PIA is a tool you can use for planning how to respond to these requests.

12.Corrections, updates and annotations

Organizations that collect, use, and disclose personal information have an obligation to ensure that the information is accurate and complete.[16] Individuals have a right to contact your organization and request to correct or update the information you hold about them. Your PIA should set out how you would accomplish this.

If you cannot correct or update the information, you must annotate the personal information with the correction that the individual requested but that you did not make.

When your organization completes a correction or update, you also have an obligation to inform all organizations that you disclosed that information to within the last twelve months. Noting who these organizations are in your personal information inventory will make identifying whom to notify easier. You should also consider and document how you will communicate these corrections, updates, or annotations to any service providers.

[15] PIPA Section 23
[16] PIPA Section 33

13.Retention

Your organization must destroy any documents containing personal information, or remove the means by which personal information can be associated with individuals, as soon as it is reasonable to assume that you have achieved the purpose for collecting the information and the information no longer has any legal or business purpose.[17] If you have made a decision that directly affects the individual, the personal information used to make that decision must be retained for at least one year so that an individual has a reasonable opportunity to obtain access to it.[18]

Your PIA should contemplate what your legal and business obligations with personal information are and establish the length of time that you will retain the record. For example, the CRA may require the retention of certain tax records for seven years. This retention period can change, as PIAs are living documents, but it is important to establish from the beginning that your organization cannot, and will not retain the personal information indefinitely.

You should note the retention period(s) in your personal information inventory.

14.Disposal

Once your retention period has expired, your organization should proceed with the secure disposal of the information. Part 4 of the PIA should examine the format of the data (digital, paper, cloud, etc.) and consider what procedures your organization will follow to destroy the data. The PIA should identify the procedures for identifying expired records, identifying their transfer to archives, or the destruction of the records, where these procedures can be located, and approximate the flow for disposing of the records within the PIA.

PARTS 5-7
COMMENTS AND SIGN-OFF

15. Privacy officer comments

Organizations are required to designate one or more individuals to be responsible for ensuring that the organization complies with PIPA.[19] This section provides an opportunity for the privacy officer to document their thoughts, comments, and opinions about the initiative.

[17] PIPA, section 35(2)
[18] PIPA, section 35(1)
[19] PIPA, section 4(3)

16. Signatures

By signing off on the document, your organization is creating internal accountability and management is accepting any risks involved in the collection, use, disclosure, storage, and access of personal information. Signing authorities should be individuals within the organization with sufficient authority to evaluate the risks on behalf of the organization and make a determination about their acceptability.

RESOURCES FOR FURTHER INFORMATION

Visit www.oipc.bc.ca/resources/guidance-documents for further guidance on how to comply with PIPA.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867
info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy