Privacy and Cloud: Guidance for MPOs

This guidance provides Ministry Privacy Officers (MPOs) with foundational knowledge related to understanding, assessing and addressing privacy considerations for the cloud. This document provides support for the privacy assessment of cloud services and an understanding of the importance of the Privacy Protection Schedule for Cloud Services (cPPS).

Although cloud services have been available commercially for some time, government is in the early stages of adoption. MPOs should be comfortable outlining the privacy risks in this document to ministry program areas. Expectation setting for ministry program areas is important to ensure that project commitments are compliant and informed.

Note that this document is focussed on privacy only. The content contains links to procurement, security and contract work, but an in depth look at these three processes is outside the scope of this guidance. As well, this document does not cover the private cloud storage services that the Office of the Chief Information Officer (OCIO) offers as those do not carry the same privacy risks.

This guidance is developed using an iterative process and will be revised based on continuous learning by Privacy, Compliance and Training (PCT) and Ministry Privacy Officers (MPOs).

How to Identify a Cloud Service

A service may be using cloud when information is not in government's Kamloops and Calgary data centres or where government information otherwise leaves the internal network. A cloud service is a service that is made available to users on demand from a cloud computing provider's server as opposed to being provided and managed by government's own on-premises data centre. This may include data centres that rely on private cloud storage following assessment by PCT and other areas of the OCIO.

If access to the system is bought (vs. buying/licensing a copy of the system that the program area/user operates independently), the service is likely a cloud service. Subscription-based and free-to-use online services are typically cloud solutions. Services where you create a username and password to log in, free email services and other free online services are often cloud based.

A key resource to help determine if you have a cloud service is the Office of the Chief Information Officer (OCIO): cloud.questions@gov.bc.ca.

Privacy and Cloud: The Basics

Before 2016, the BC public sector rarely had the opportunity to consider cloud services because they were not "data resident" (i.e. in Canada). In 2016 this landscape changed because major cloud infrastructure providers opened data centres in Canada that appeared to be "data resident." Although cloud vendors may provide data centres in Canada, this does not necessarily mean that all the technology a service relies on is offered from the Canadian data centre(s). This must be assessed, and the remainder of this document will support you to do that.

It is also important to distinguish data residency from data sovereignty. The following section illustrates the difference and discusses other key areas in cloud where there are specific privacy considerations. As MPO, you will need to explain these key areas to your ministry program area prior to and during cloud adoption for their business area. Understanding these risks will help the program area's Executive make an informed decision.

Data residency (location of data)

Data residency is achieved when personal information is stored and accessed in Canada in compliance with FOIPPA section 30.1. This means that data centres must be in Canada and that the cloud service must be architected to ensure personal information remains in Canada. For example, a cloud service provider that meets residency requirements will locate its infrastructure and backup infrastructure in Canada. A cloud service may be offered from a Canadian region (sometimes referred to as "geo" or "availability zone"); however, this does not mean that all of the services offered within the cloud service occur within the Canadian geo/availability zone only. Assessment of the technology is required to confirm that no unauthorized disclosures will occur.

It is important to assess the cloud service providers proposed routing/transmission. In particular, does access or storage outside Canada happen at any point? If so, assess for compliance with the new FOIPPA amendments regarding temporary processing and metadata (33.1(1)(p.1) and (p.2)).

Attention should be paid to the cloud service providers' access to personal information. If standing access is available to non-Canadian cloud service providers, this will not be authorized. Assessment of access outside of Canada is required to demonstrate data residency. Collaborative solutioning with the ministry program area and cloud service provider may be required (i.e. to develop or architect alternative access controls).

Note that there are many reasons that personal information can be disclosed outside of Canada in compliance with FOIPPA. Some of those reasons support cloud technology:

- Information may be disclosed outside of Canada for temporary, technical maintenance in accordance with section 33.1(1)(p) of FOIPPA.
- Information may be disclosed outside Canada for temporary processing in accordance with section 33.1(1)(p.1) of FOIPPA. This provision sets limits on that disclosure, including:
    - The processing cannot involve intentional access by a human.
    - The processing cannot result in storage of personal information outside of Canada, unless otherwise specified.
    - Where the processing happens outside of Canada, the disclosure must be for the minimum amount of time necessary.
- Information may be disclosed outside Canada if the personal information is metadata that is generated by an electronic system and that describes an individual's interaction with the system in accordance with section 33.1(1)(p.2) of FOIPPA. This provision sets limits on that disclosure, including:
    - Where practicable, any identifiable information in the metadata is removed or destroyed.
    - Where the disclosure is to a service provider, there is a contractual prohibition on using or disclosing the information further.

As the MPO, you can determine if these disclosure authorities apply. PCT is available to help.

The cPPS contains particular content that supports transparency in communicating privacy obligations to cloud service providers. There are specific access limitations drafted with support and on the advice of Legal Services Branch (LSB).

Data sovereignty (authority/control over the data)

Distinct from data residency, data sovereignty refers to authority or control over the personal information in the ministry's control.[1]

If the cloud vendor (or the vendor's subcontractor, including a third party hosting provider[2]) is a non-Canadian company, data sovereignty will likely be an issue to address even when the vendor can establish data residency (e.g. the cloud vendor has data centres in Canada but is a U.S. company). This arises because the law in some foreign jurisdictions enables those governments to make a legal demand for information that a vendor from that country has in its system (i.e. a government may have the legal ability to force companies within its jurisdiction to provide it with information regardless of the information's country of origin). In this way, a non-Canadian vendor could have a "conflict of laws" issue should the vendor's own government make such a legal demand for the information. Therefore, if a non-Canadian company is a cloud service provider (or the subcontractor of a service provider), the ministry needs to address risks associated with data sovereignty.

The cPPS contains contractual protections that protect against foreign demand in a manner that non-Canadian cloud service providers should be able to accept. This language has been drafted with support from and on the advice of LSB.

Service provider relationship

In the cloud environment, FOIPPA terminology (e.g. collection, use, disclosure) is not a natural fit for cloud vendors. Cloud vendors who contract with a ministry may not realize they are service providers of that ministry – they simply provide a cloud service[3] or see themselves more as "processors" instead of service providers. Though this may be accurate from a business standpoint, this is not the case under BC privacy legislation. Cloud contractors are service providers under FOIPPA, and by extension, the privacy protections required of a government employee extend to the service provider (cloud provider) and their contractors.[4]

---

[1] "Control" (of a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure. Refer to FOIPPA Policy Definitions.

[2] Definition from the Privacy Protection Schedule for Cloud Services: "Third Party Hosting Provider" means a third party that provides a platform or hosting service through which the Contractor delivers the services under the Agreement and to whom personal information is not accessible and as such, for the purposes of this Schedule, is not considered a subcontractor.

[3] Note that some cloud services are offered under a reseller model. The reseller model presents unique challenges to cloud assessment and at this time, early engagement with PCT is recommended.

[4] The definition of "employee" in Schedule 1 of FOIPPA includes "service provider," and employees of a public body are subject to FOIPPA.

"Custody" and "control" are FOIPPA terms not easily applied to the cloud environment because of how cloud services are used. Under FOIPPA, the cloud service provider has custody of the personal information while the ministry retains control.[5]

As MPO, you can help the ministry program area in working with a cloud vendor by advising that the service provider needs to understand their obligations under FOIPPA, including data residency, data sovereignty, custody and control. This can be done verbally or drafted as part of the solicitation documentation for a Request for Proposals (RFP) in collaboration with PCT. PCT is developing plain language privacy requirements that can be included in procurement solicitation documentation.

The cPPS provides clear contractual language that ensures the cloud service provider is obligated to adhere to FOIPPA. It also contains language specific to the "flow down" of FOIPPA obligations where it has subcontractors who handle personal information. Finally, there are specific carve outs for a "Third Party Hosting Provider." This is a defined term in the cPPS.[6] The cloud service provider does not have to flow down terms to third party hosting providers if that party does not access personal information. If their hosting provider does access personal information, that cloud service provider is a subcontractor of the Province's service provider and therefore, FOIPPA must flow down to them. It is likely that this will require specific privacy assessment.

When the vendor cannot accept the "Third Party Hosting Provider" terms (i.e. the third party hosting provider can access personal information), there are three options:

1. The vendor will need to flow down contract terms to the third party hosting provider (difficult for large platform and infrastructure providers);
2. Government will need to work with the vendor on technical options to prevent the third party hosting provider from accessing personal information; or
3. In the absence of 1 or 2, government must assess the risk of non-compliance (i.e. logical assessment of sensitivity of the personal information, legal/PCT consultation, Executive briefing).

FOIPPA and Cloud: Two different ways of thinking

Service provider vs. non-service provider: In accordance with FOIPPA, cloud vendors are service providers and the ministry's FOIPPA obligations apply to them.

Customer data vs. personal information: The cloud vendor may only identify information as "customer information" or "customer data." They may not distinguish between personal and non-personal information. If this is the case, it is important that customer data/customer information be treated with the same protections as personal information.

Non-personal information vs. anonymized data: The cloud vendor may not immediately recognize that personal information that has been anonymized may require specific protections. The protections the Province requires for anonymized data is different from information that was never personal to begin with (e.g. data about a system's health like battery level).

---

[5] "Custody" (of a record) means having physical possession of a record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security. Refer to FOIPPA Policy Definitions.
For definition of "control," see previous footnote.

[6] See footnote #2.

Cloud vendor privacy protections vs. FOIPPA: It is important to recognize that a cloud service provider's compliance to a high privacy standard (e.g. Federal "Protected B," ISO27018, GDPR, etc.) does not mean they will by default meet the requirements of FOIPPA.

Privacy and Cloud: Outstanding Risks

The following risks will require specific assessment and may require intervention. The Privacy, Compliance and Training Branch (PCT) is available to help. Early engagement with PCT will ensure that they are able to support you through the most appropriate stage (e.g. RFP development; proponent evaluation; contract negotiation or finalization; Privacy Impact Assessment (PIA)).

Data residency, data sovereignty and foreign demand

Data residency and data sovereignty must be assessed, and risks must be mitigated through technological and contractual protections.

Service providers

The cloud service provider must agree to terms that flow contractual protections from the vendor to any subcontractors who access, collect, create, use, disclose, retain, dispose of, etc. personal information.

IaaS: Different privacy risks

The privacy risks associated with cloud are variable depending on the specific nature of a cloud solution. There will be certain risks and mitigation strategies for a SaaS vendor who does not allow the third party hosting provider access to any personal information. These risks will differ when a ministry is looking to consume services directly from a PaaS or IaaS provider. Early intervention and collaboration with PCT, LSB and security (either Information Security Branch, or the Ministry's Information Security Officer) are key strategies to support the development of risk mitigation strategies that are tailored to the specific cloud service provider. Enterprise level and infrastructure services should come directly from the OCIO.

Collaboration is Key

Engage the Ministry Information Security Officer (MISO) and/or the Information Security Branch (ISB) as early as possible. PCT recommends early engagement with the MISO and/or ISB on all cloud files. Note that PCT will request that any PIA assessing cloud services be reviewed and signed by the MISO given the subject matter expertise required to evaluate "reasonable security" (FOIPPA section 30) in the cloud context.

Collaborative Partners

Cloud File Stage	**Collaborative Partners**
Procurement	MPO, Program Area, Legal Services Branch (LSB), ministry procurement specialist and/or Procurement Services Branch (PSB), PCT (involved until a privacy procurement tool is in place – this is in development)
Cloud assessment	MPO, Program Area, MISO and/or ISB, PCT (involved to support: SME knowledge transfer to MPOs, support assessment of cloud compliance)
STRA	MPO, MISO and/or ISB
Contract (privacy terms)	PCT (involved where deviation from the cPPS is required per Core policy), Program Area, LSB, MPO (involved at their discretion), Service Provider

Privacy at Multiple Phases of a Cloud Project

Planning and/or procurement

If relevant, ensure that privacy requirements included in the procurement language adequately address privacy concerns in the cloud context. In addition to the approved cPPS, PCT is working with cross-government partners to develop additional, plain language privacy requirements to include in a ministry procurement for cloud services. In the interim, contact PCT for support and to ensure you have access to the most up to date strategy and best practices. You may also want to support your program area to connect with procurement and legal experts (Procurement Services Branch (PSB) and Legal Services Branch (LSB)).

Evaluation and/or PIA

The ministry must conduct a Privacy Impact Assessment (PIA). The timing of when to complete the PIA will vary (though always before the project or program goes live).

The ministry may also need to do other evaluations during other project phases. One example is evaluation of the lead proponent during a procurement. The MPO can work with the ministry program area to gather information from the proponent to inform potential privacy showstoppers (e.g. not data resident). The Guideline for Assessment (currently in development) is a useful guide.

The ministry will also need to conduct a Security Threat Risk Assessment (STRA). For cloud assessments, the STRA and PIA support one another. For example, you will need to assess access controls in both, and it can be helpful to look at these two deliverables as a collaborative effort because both disciplines apply a different lens.

When assessing a program that intends to rely on a cloud service, the PIA must assess a) the ministry program; and b) the cloud service, including the architecture and each of the services the cloud vendor is expected to provide (including failover technology) in addition to future services that may be required. Given the nature of the technology (variables related to SaaS/PaaS/IaaS and mitigations that are specific to the technology; the contract; and the type/volume/sensitivity of personal information), the assessment will always be unique to that particular project.

There can be many layers to cloud service offerings. All components of the technology stack must be considered. Some layers may require privacy assessment and contractual protection (e.g. where the IaaS can access personal information) and others may not (e.g. where the IaaS is provided by a third party hosting provider who does not access personal information – and this has been assessed and confirmed in contract – or where the IaaS is provided by the Office of the Chief Information Officer's (OCIO) approved on-premise private cloud).

Expectations for a cloud PIA:

- The PIA must include assessment at a technical level to determine potential risks associated with disclosure, storage or access of personal information outside of Canada, etc.
- The PIA should explicitly document how the vendor intends to address issues associated with data residency, data sovereignty and their service provider relationship (including with the vendor's own subcontractors). All three of these issues carry risks to privacy, and the PIA is the tool that documents the risks and associated mitigation strategies.

- Refer to the Guideline for Assessment (currently in development) to help with completion of the PIA.

The PIA is used to assess and document risks, the associated mitigations and outstanding risks (e.g. foreign demand) to ensure that the ADM responsible for signing the PIA has been briefed on the complexity of the problem.

Together, the PIA, STRA and contract demonstrate due diligence and address compliance of the solution. For this reason, the PIA may require final contract language to be included. Should PIA sign off be an important milestone for the project and/or Executive approval, please discuss this with PCT.

PCT will support you as the MPO to determine whether to engage with the Office of the Information and Privacy Commissioner (OIPC). Factors that will inform PCT's advice on this issue include: whether the particular technology solution has been brought to the OIPC before; whether comparable technical risk mitigation and/or contract protections have been brought to the OIPC before; and sensitivity and/or scale of the personal information.

The privacy and security requirements that were committed to in the PIA are now a list of actions to take for implementation of the cloud service. The project team can use these outputs to set up the cloud service.

Privacy Tools and How They are Related

Tool	Related Tool	Relationship
Procurement privacy requirements (solicitation documentation)	Contract	Privacy language in the bid/posting procurement phase will carry over to the contract phase. If the requirements do not match the final contract, there may be an increase to the procurement risk for the Province.
Contract	PIA	Privacy language in the contract will inform mitigation to risks identified in the PIA.
PIA	Contract	The PIA will identify privacy risks and mitigation strategies. Some of those mitigation strategies will be reflected in the contract language.
STRA	PIA	Assessment of the service at a technical level will help inform PIA responses to access, storage, processing, etc. In addition, if risks are discovered in the STRA (e.g. inadequate application of encryption), these can be addressed and mitigated in the PIA.

When Section 33.1 Applies (Excluding Section 33.1(1)(p))

An in-depth privacy assessment of the project is not required if the project has the authority to disclose information under FOIPPA section 33.1 (other than with section 33.1(1)(p), (p.1) and (p.2)). For example, where another act authorizes the disclosure (section 33.1(1)(c)) or where the individual consents to the

disclosure (section 33.1(1)(b)).[7] In these cases, the privacy assessment of the cloud technology does not need to be as technically deep because there is a FOIPPA authority to disclose personal information outside of Canada.

Reasonable security must still be ensured; therefore, PCT will request that the MISO sign the PIA.

Finally, collaboration with procurement specialists (e.g. Procurement Services Branch (PSB)) during the procurement phase is likely necessary to ensure compliance with Chapter 6 of the Core Policy & Procedures Manual.

Guideline for Assessment

The Guideline for Assessment is a separate document and is currently in draft. Please contact PCT for support.

The guideline can be used in the following circumstances:

- **When evaluating a vendor during procurement**
- **Prior to finalizing the contract**
- **When completing the PIA**

Contract

Ensure appropriate contractual controls are in place.

- The BC government uses the Privacy Protection Schedule for any contracts that involve personal information. Note that a non-Canadian cloud service provider will likely be unable to agree to the terms in the Privacy Protection Schedule and alternate terms may need to be agreed upon.
- In accordance with Chapter 6 of the Core Policy & Procedures Manual, alternate language to the standard Privacy Protection Schedule must be approved by PCT.
- For cloud projects that involve personal information, PCT has developed a Privacy Protection Schedule for Cloud Services (cPPS) that replaces the standard Privacy Protection Schedule in contracts. The cPPS strategically addresses numerous issues that have consistently required attention in cloud negotiations where personal information is involved.
- Early collaboration: Ensure that PCT and LSB are engaged in conversations with the program area and the service provider at the earliest point and concurrent with drafting of the PIA and STRA.

Executive Briefing

While it is possible to achieve compliance with FOIPPA, there may be outstanding risks, and ministry Executive should be made aware of the risks before the ministry enters into a contract. Note that PCT is available to support the MPO and/or ministry program area in Executive briefing. PCT will seek

[7] Consent may be a good model for low sensitivity personal information, where a reasonable person is likely to consent. You will want to consider alternatives for those who do not consent.

confirmation that Executive has been briefed, at minimum through the PIA process. PIA will seek confirmation of this before approving amendments to the Standard PPS.

Executive briefing should be tailored to the specific, outstanding risks of a cloud file (based on risks identified in the PIA and mitigated both technically and contractually). Risks may include the following but will be confirmed during the assessment:

- U.S. legislation, *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), provision(s)
    - LSB's FOIPPA counsel will assess the impact of this risk.
- Status of risk mitigation regarding service provider relationship, data residency and data sovereignty
    - Status of access controls
        - Brief Executive on access controls that present outstanding risk and provide the pros and cons of accepting that risk.
    - Status of data protection controls
        - The architecture of a system may provide data protection. Brief Executive on data protection controls that present outstanding risk and provide the pros and cons of accepting that risk.
    - Status of contractual controls

Revision History

Version	Date	Notes
1.0	August 13, 2019	Draft reviewed by Cloud Privacy Working Group and approved by Privacy, Compliance and Training Executive Director.
1.1	September 3, 2019	Updated cPPS portions following Executive decision.
1.2	December 30, 2019	Added content regarding new FOIPPA amendments 33.1(1)(p.1) and (p.2)