CLOUD COMPUTING FOR SMALL- AND MEDIUM-SIZED ENTERPRISES:

Privacy Responsibilities and Considerations

Cloud computing is the delivery of computing services over the Internet, and it offers many potential benefits to small and medium-sized enterprises (SMEs). For example, implementing information technology solutions and platforms can be complex and costly for SMEs. Cloud computing can often help ease this burden by enabling SMEs to access services that they might not have the money or resources to implement or support on their own. Many organizations may employ cloud computing solutions as part of their overall business strategy, allowing them to focus on their core business.

Organizations may turn to cloud computing services for data processing, storage and backup, to facilitate productivity, for accounting services, for communications, or for customer service and support. There are privacy implications, however, if personal information is being handled by a cloud provider.

The Office of the Privacy Commissioner of Canada (OPC) has developed an *Introduction to Cloud Computing*, which provides general information on cloud computing and the privacy challenges it presents, and includes answers to a number of frequently asked questions.

This guidance document, prepared jointly by the OPC and the Offices of the Information and Privacy Commissioner of Alberta and British Columbia is specifically intended to help SMEs understand what their privacy responsibilities are and to offer some suggestions to address privacy considerations in the cloud. This document should be read in conjunction with the *Introduction to Cloud Computing* document.

Other related resources are referenced at the end of this document.

Are you already in the cloud?

As a first step, SMEs should examine their organization to determine if any of their business activities already involve outsourcing personal information to a cloud computing service. Frequently, organizations find that employees have already moved personal information to a cloud service without IT staff or management being aware. For example:

- Do employees use a cloud-based e-mail service for business correspondence?
- Do employees use an online service to collaborate on documents containing personal customer information?
- Can client databases be accessed online from any location?

Consider the risks & benefits of moving to the Cloud.

Cloud computing is a type of outsourcing. While cloud computing may provide efficiencies, as noted above, there are potential risks related to the use of a cloud service provider. If an organization chooses to outsource personal data for processing or other services to a cloud service provider, it remains accountable for protecting its customers' personal information and it must be transparent about its information management and privacy practices.

Organizations must ensure they fully understand their obligations under Canada's private sector privacy legislation, including those under certain provincial privacy legislation[1], and they need to carefully assess the risks against the benefits. Organizations considering a cloud computing service should carefully consider *what* information will be stored in the cloud and *why*. Organizations must consider the sensitivity of the personal information and carefully assess all the risks and implications involved in outsourcing personal data to the cloud. This assessment should also take into account whether the cloud is a public cloud, community cloud, private cloud or hybrid cloud, as defined in the OPC's *Introduction to Cloud Computing*.

The sensitivity of the information, the type of cloud, and the contractual arrangements should all play a key role in an organization's decision to move, or not to move, personal information to the cloud. It may be beneficial to consult a professional for assistance in assessing the risks of using a cloud service provider.

Take accountability into account. What does the contract say?

Under Canada's private sector privacy legislation, an organization that collects personal information from an individual is accountable for the personal information even when it is outsourced for processing to third-party providers. What this means is that all businesses in Canada, regardless of their size, are ultimately accountable for the personal information they collect, use and disclose even if they outsource personal information to a service provider that operates in the cloud.

Organizations sometimes find that cloud providers present "take it or leave it" contracts. In other words, the provider sets the parameters of the relationship, and the contracting organization is required to go along with it in order to use the service. This tends to be the case with free online services offered by cloud providers. The concern is that the terms of service that govern the relationship with the cloud service provider sometimes allow for more liberal usage of personal information and retention practices, and these standard contract clauses may not be sufficient to allow SMEs to meet their privacy obligations. Moreover, it may be problematic if the cloud provider is able to unilaterally change the agreement, limit its liability for the information, and/or subcontract to various other providers.

[1] The *Personal Information Protection and Electronic Documents Act* (PIPEDA) and substantially similar provincial laws, including, Alberta's *Personal Information Protection Act* (PIPA); and British Columbia's *Personal Information Protection Act* (PIPA). Although the specifics of all three pieces of legislation may differ, they are all deemed to be substantially similar in content and contain the same fundamental principles. In some provinces, an organization may be subject to specific notification requirements in accordance with provincial privacy legislation. In Alberta for example, there are specific breach notification requirements and requirements to notify individuals when personal information is transferred to a service provider located outside of Canada.

SMEs in particular might be more likely to encounter a 'take it or leave it' situation than larger organizations that have more resources to push back on such contracts, or set up a private cloud. Still, the accountability remains with the outsourcing organization even if the service is free, or if the cloud provider sets a "take it or leave it" contract. As noted in the *Introduction to Cloud Computing – FAQs*, any organization using a cloud service must carefully review the cloud provider's terms of service and ensure that the personal information it entrusts to the provider will be treated in a manner consistent with its privacy obligations under relevant privacy legislation. In short, SMEs must use contractual or other means to ensure that personal information is appropriately handled and protected by the cloud provider. The bottom line? If you are not comfortable with what a particular cloud provider is proposing, you should not transfer personal information entrusted to you by your customers to that provider. You should push back, or take the time to shop around for a better solution. Check out other providers and confer with other similar businesses or your industry association to see what options may be available.

For additional guidance on accountability, consult *Getting Accountability Right with a Privacy Management Program*, which was prepared jointly by the Offices of the Information and Privacy Commissioners of British Columbia and Alberta, and the Office of the Privacy Commissioner of Canada.

Is the cloud secure?

Security in the cloud is of paramount importance. Massive online databases are attractive to cybercriminals, and Internet services have proven to be difficult to protect. Organizations must protect personal information with safeguards appropriate to the sensitivity of the information they handle. Tools such as Privacy Impact Assessments (PIA) or Threat Risk Assessments (TRA) could be valuable to help make assessments of safeguards. In order to ensure that personal information is protected, organizations using cloud computing services should:

- **Limit access to the information and restrict further uses by the provider.** Set parameters for restricted access and use of personal information that is appropriate for the context and sensitivity of the information. Find out if personal information will be segregated or stored in the same database as information from the cloud provider's other clients. Ensure access to personal information is only granted to those who need it to do their job. Ensure that access to personal information is logged in protected audit trails. Do *not* assume that the provider's general terms of service or policies will be adequate to establish such restrictions, review them carefully.

- **Ensure that the provider has in place appropriate authentication/access controls.** Stronger methods of authentication are recommended, such as multi-factor authentication[2]. The level of authentication should be commensurate with the risk to the personal information being protected. Ensure there are procedures and technical controls to manage who has access rights to the personal information.

- **Manage encryption.** Understand what type of encryption method is being used and identify where data is encrypted or unencrypted at each stage (e.g., data in transit, data at rest). Conduct an assessment of the risks associated with any lack of encryption.

[2] Refer to our *Guidance on Identification and Authentication* for an explanation of multi-factor authentication.

Determine if the encryption method is adequate and the access to encryption keys is properly managed. Risks may be reduced if organizations encrypt personal information before it is sent to the cloud provider.

- **Ensure that there are procedures in place in the event of a personal information breach or security incident.** These should include technical and organizational measures that will be implemented in the event of accidental or deliberate loss, or unauthorized access or disclosure of personal information. Ensure there are provisions in the agreement with the cloud provider that specify when it will provide notification to the organization in the event of a security breach. Organizations subject to breach notification requirements will want to ensure the contract is clear about when the cloud provider is to provide reports on breaches in order for it to meet its legal obligation[3].

- **Ensure that there are procedures in place in the event of an outage to ensure business continuity and prevent data loss.** Business continuity plans should be clearly documented in the contract.

- **Ensure periodic audits are performed.** It is important for an organization to have some measure of oversight over a cloud provider's policies and practices. Ensure the cloud provider logs all accesses and uses of personal information. Audits should be conducted periodically to inspect access logs and confirm that physical locations where personal information is processed and stored are inspected. Organizations should verify practices and procedures to ensure the provider is handling personal information in accordance with the agreements in place and request evidence of effective auditing and timely response to security incidents.

- **Have an exit strategy.** Ensure the termination procedures permit the transfer of personal information back to the organization and require that the cloud provider securely delete all personal information within reasonable and specified timeframes.

If your organization needs help evaluating its personal information protection readiness, you can consult the *Securing Personal Information: A Self-Assessment Tool for Organizations*, which was prepared jointly by the Offices of the Information and Privacy Commissioners of British Columbia and Alberta, and the Office of the Privacy Commissioner of Canada.

State your purpose. Do you have your customer's consent?

An organization needs to ensure that appropriate consents have been obtained if it plans to outsource personal information to a third-party cloud provider. If an organization has obtained an individual's consent to collect and use personal information for a specific purpose, it does not need separate consent when outsourcing to a cloud provider to process the information for the *same purpose* outlined at the time of collection. Ideally, at the time of collection, organizations should inform customers in clear and understandable language that their information may be processed by a third-party service provider.

[3] In some provinces, an organization may be subject to specific breach notification requirements

Establish limits. Have you specified what the cloud provider can do with the data?

Organizations need to be cautious about "function-creep", where a cloud provider may use the information for purposes other than those for which it was collected. Organizations need to maintain control over personal information that is sent to a cloud provider, and take steps to prevent and limit secondary uses of personal information. However, if there is concern that the contractual arrangement would permit the cloud provider to use the information for other reasons (such as targeted advertising) *separate consent* would be required from customers for any secondary or new uses of their personal information.[4]

Before moving personal information to the cloud, organizations need to:

- **Clarify what, if anything, the prospective cloud provider will do with the information.** Will it analyze the data for its own purposes? Will it sell it? Will it sub-contract certain activities related to the cloud service? Will the data be segregated or stored with data from the provider's other clients? Ensure that these activities will not result in a violation of privacy obligations and raise any concerns you have directly with the cloud service provider.

- **Seek customers' consent for new uses of their personal information.** If the cloud provider purports to use the personal information for purposes other than the specific purposes for which the personal information was initially collected, then separate consent for that new use is required. If customers do not consent, or revoke consent, you need to ensure that you can comply with their requests.

- **Always keep in mind the reasonable expectations of the individual.** What would your customers think of the proposed uses? You need to maintain the trust of your customers, while providing them with the best possible service and protection.

Transparency is key. What will your customers expect?

Individuals will expect that their personal information is protected, regardless of where it's processed or stored, and will also expect an organization to be transparent when personal information is outsourced to a cloud provider. Organizations should use clear and understandable language to inform individuals that their personal information will be transferred to a cloud provider, that their personal information may be stored or processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction.

[4] However, there are limited exceptions that may apply in certain circumstances, for example, when new uses or disclosures are authorized by law.

The cloud crosses borders. Do you understand how the law will apply?

Canada's private sector privacy legislation does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing.[5] However, organizations should consider the sensitivity of the personal information they plan to outsource and evaluate the potential risks that may occur when moving personal information outside the country. Organizations need to recognize that personal information that is transferred to another country is subject to the laws of that jurisdiction. In the case of cloud computing, data that is outsourced may be physically located in several jurisdictions. Moreover, the cloud provider's backup servers could be in a different physical location than the primary servers. It is important to understand where the data will reside to fully comprehend the legal regimes for protecting personal information, and the circumstances under which data may be accessed by foreign courts, government agencies, and law enforcement.

It is also important to be aware of the limitations for obtaining judgements and enforcing contracts. No contract, no matter how well crafted, can override the laws of the foreign jurisdiction. *Moreover, generally an organization can only enforce the provisions of a contract against the other party to the contract, and not third-parties.* In a foreign jurisdiction, obtaining judgements to enforce contracts may be difficult and costly for the outsourcing organization. It may prove to be equally difficult to enforce a judgement in a foreign jurisdiction.

For additional guidance on transborder data flows, see the OPC's *Guidelines for Processing Personal Data Across Borders*. These considerations apply whether an organization is moving data into the cloud, or otherwise transferring personal information across borders.

It's important to maintain control. Are you in the driver's seat?

Organizations have obligations under privacy laws that include enabling customers to access their personal information, request corrections, and resolve issues and complaints. Accordingly, an organization must ensure that its relationship with the cloud provider allows it to meet these obligations under privacy law. For example, the organization must have the ability to access data at any time (including backups and archives), make corrections, and investigate any allegations of non-compliance with privacy obligations. In the event of a breach, organizations will also want control over the procedures to notify affected individuals.

Outsourcing the handling of personal information to a cloud provider means that the cloud provider will have custody of the personal information. As such, an organization needs to be cautious that it does not lose control of the personal information transferred to the cloud provider. Maintaining control means that data ownership is clearly defined in the contract and includes statements about what the provider can do with the personal information and what will happen to the personal information if the provider ceases to operate. Part of maintaining control also means that an organization has the ability to terminate the contract, retrieve the data from the cloud provider, and have the cloud provider attest that no personal information is retained in its systems, or any of its subcontractor's systems.

[5] However, it's important to understand specific legal obligations that exist under some provincial privacy laws. For example, Section 13.1 (2) of Alberta's *Personal Information Protection Act* requires organizations to provide notice to individuals at or before the time of collection of their personal information, if their personal information will be transferred to a service provider located outside of Canada. The notice must be in a form and contain the information specified section 13.1 (3) of Alberta's *Personal Information Protection Act*.

Portability is a key component of control; portability refers to the ability to move data across different platforms with minimal integration issues. If the provider uses proprietary formats it may be more difficult for an organization to move the data back in-house or to another provider.

Organizations might also find it useful to use a cloud provider that has a person designated with responsibility for privacy. This person would ideally be identified in a contract and be accessible should the organization have any questions or concerns, or need to re-evaluate policies and procedures.

Make an informed decision.

Organizations must take care to fully assess the benefits, risks, and implications for privacy when considering a cloud computing solution. In a separate annex we have compiled a list of some* key questions that organizations should take into account when shopping for a cloud computing solution.

For more information and guidance, please see:

1) *Fact Sheet: Introduction to Cloud Computing:*
    - http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.asp

2) *Reaching for the Cloud(s):*
    - http://www.priv.gc.ca/information/pub/cc_201003_e.asp

3) *The Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing:*
    - http://www.priv.gc.ca/resource/consultations/report_201105_e.asp

4) *Guidelines for Processing Personal Data Across Borders:*
    - http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp

5) *Securing Personal Information: A Self-Assessment Tool for Organizations* (prepared jointly by the Offices of the Information and Privacy Commissioners of British Columbia and Alberta, and the Office of the Privacy Commissioner of Canada):
    - http://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

6) *Guideline on Identification and Authentication:*
    - http://www.priv.gc.ca/information/guide/auth_061013_e.asp

7) *Getting Accountability Right with a Privacy Management Program:*
    - http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp

* This list is intended as a guide and is *not an exhaustive risk analysis*. It is an organization's responsibility to fully assess the risks/benefits that are specific to its context, and in some cases, it may be beneficial to consult a professional.

Cloud Computing Key Questions

Why the cloud?

- What information do you plan to outsource and why?
- How sensitive is the personal information?
- What are the benefits and what are the risks and privacy implications for your customers?
- What are the risks to your company?
- What are your privacy obligations under relevant privacy legislation?
- What are the implications for your customers if their data is compromised?

Accountability – contract clauses

- Does the contract address all aspects of privacy compliance?
- Does your organization control the information, including how it is used, how it is accessed, and how long it will be retained?
- Who has control of the personal information if your organization, or the cloud provider, ceases to operate?
- Will the cloud provider subcontract services, which may involve access by, or transfer of information, to another provider?
- Will you be able to review the provider's processes and procedures?
- Has the cloud provider claimed limited liability in the event of a breach?
- Are there termination procedures that will allow you to recover personal information?
- Do the termination procedures require the cloud provider to securely delete personal information within reasonable and specified timeframes?

Security

- Will the data be segregated or stored with data from other organizations that use the same cloud provider?
- When and how is the information encrypted? Is the method adequate?
- What are the risks at the points where information is not encrypted?
- What are the procedures for authentication? Are they adequate relative to the sensitivity of the information?
- Are there policies and procedures that restrict access to the data?
- What are the technical and organizational measures that will be implemented in the event of accidental or deliberate loss of data, or unauthorized access or disclosure?
- What are the notification procedures in the event of a security breach?
- Do you have the ability to obtain evidence of effective auditing?
- What is the disaster recovery plan?
- Have you outlined an exit strategy?

Secondary uses

- What will the prospective cloud provider do with the information?
- Will the provider analyze the data for its own purposes?
- Could the provider sell the information?
- Will the provider use or allow access to the information for targeted advertising?
- Will any of these secondary uses result in your organization's non-compliance with applicable privacy laws?

Knowledge, Consent and Transparency

- Are your customers aware that you will be sharing their information with a third party? Where applicable, have you met your notice requirements?
- Will the cloud provider process the information for the same purpose for which you collected it? Do you have your customers' consent?
- Would your customers reasonably expect their information to be used for that purpose?
- If this is a new purpose, what is your plan to advise your customers and obtain additional consent?
- Do you have a plan to respond to cases where customers do not consent or withdraw consent to a new use?

Control, Accessibility and Portability

- Is there a risk that the cloud provider could refuse to give your data back to you?
- Does your relationship with the cloud provider allow you meet obligations for allowing individuals access to their personal information?
- Do you control the notification procedures in the event of a breach?
- Will the data stored by the cloud provider be portable? Will you be able to transfer the personal information back in-house or to another provider?
- Does the cloud provider have a designated privacy person that is accessible?
- Do you have the ability to access data at any time, make corrections, and investigate any allegations of non-compliance with privacy obligations?
- Will you lose control of personal information to your provider's subcontracted providers?

Jurisdiction and access

- Where will the data be stored?
- What are the risks in outsourcing to that jurisdiction?
- What foreign entities could potentially have access to the information?
- What are the cloud provider's policies with respect to access to information requests?
- Will a warrant or subpoena be required prior to granting access to foreign courts, government agencies, and law enforcement?
- Will the cloud provider inform your organization if data is requested or disclosed pursuant to a legal requirement?
- Will the cloud provider seek direction from your organization prior to sharing information with others, including law enforcement?