Table of Contents

Addressing compliance with privacy laws for cloud-based services through persistent encryption and key ownership ........................................................................................................................................... 3

Section I: Vaultive Response to PIPEDA, PIPA (Province of Alberta), PHIPA (Province of Ontario) and FIPPA Requirements ........................................................................................................................................... 4

Section II: Data Residency and Residency of Controls ................................................................................................................................................................................. 9

Vaultive Response: Maintaining Data Privacy and Control Residency ................................................................................................................................. 10
Addressing Data Control and Compliance with Canadian Privacy Regulations for Cloud-based services:

The adoption of cloud computing presents a new set of compliance concerns and need for best practices guidelines under privacy laws applied to both Canadian government bodies and organizations in the private sector. The Government of Canada and provincial governments have been required to manage the privacy of personal information since the passage of the Privacy Act of 1983. With the development of online commerce, requirements for the protection of personal information were extended to private sector organizations holding electronic records of personal information when the Personal Information Protection and Electronic Documents Act of 2004 was passed.

The privacy laws and legislation share a set of common principles that relate to accountability, technical safeguards and limiting disclosure of personal information, at least in the context of this discussion. As cloud computing adoption grows, concerns about the integrity of safeguards for the privacy of personal information have intersected with anxiety over the implications of trans-border data flow and data residency issues that could be viewed as at odds with Canadian privacy requirements. This evolving landscape is catalyzing the initial definition of best practices related for the ownership and control of data processed in third-party environments.

Addressing compliance with privacy laws for cloud-based services through persistent encryption and key ownership

At the heart of the concerns that bring compliance under consideration is how organizations can continue to maintain control and protection of personal information, even when the information resides on a third-party service. Vaultive's platform is designed to complement existing cloud service provider security safeguards through an additional layer of data control capabilities based on persistent encryption and retention of the encryption keys by the organization held accountable for privacy protection. These data control capabilities enable organizations to satisfy the requirements for accountability and technical safeguards, specifically in the area of encryption. Vaultive's proxy-based approach enables organizations to seamlessly extend the trusted enterprise boundary through advanced encryption-in-use capabilities and preserve application functionality through platform extensions for Office 365 and Hosted Exchange services.

In line with the Cloud Security Alliance's updated security guidance covering best practices for migrating data to the cloud, Vaultive's enterprise-grade cloud data encryption solutions enable customers to encrypt data-at-rest, data-in-transit and data-in-use in the cloud.

Microsoft has committed to providing Office 365 and Hosted Exchange customers the performance, scalability, security and service levels business customers expect, as well as ongoing investment in security processes and technologies. Vaultive's data control and encryption capabilities complement access management technologies for cloud-based services, such as federated identity supported by Microsoft technologies such as Active Directory Federation Server.

This document provides an overview of how Vaultive's technology addresses the security, privacy and accountability requirements as defined by current Canadian privacy law, related to both government institutions and commercial organizations, specifically in the context of cloud-based services. The Personal Information Protection and Electronic Documents Act (PIPEDA) and related Personal Information Protection Act (PIPA) legislation as declared by provincial legislatures in Alberta, British Columbia, Ontario and Quebec is directed primarily at commercial organizations, while the Privacy Act of 1985 and the Freedom of Information and Protection of Privacy Act (FIPPA) covers federal and provincial organizations.

Section I of this document also serves to illustrate how Vaultive can address the technical safeguards and accountability requirements as defined in the various laws. Section II addresses how Vaultive's key management and proxy-based approach enables Canadian organizations to manage border data flow and maintain residency of data controls.
## Section I: Vaultive Response to PIPEDA, PIPA (Province of Alberta), PHIPA (Province of Ontario) and FIPPA Requirements

<table>
<thead>
<tr>
<th>PIPEDA Requirement</th>
<th>Description of Controls</th>
<th>Vaultive Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.3 Principle 1 – Accountability</td>
<td>&quot;An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.&quot;</td>
<td>Vaultive's design goal is to deliver a platform that directly addresses the requirements for ownership and control of personal information under an organization's custody that resides or is processed on cloud-based services. Through deployment of the Vaultive proxy, organizations can encrypt data before it leaves the trusted network, while enterprise IT retains the encryption keys. Based on advanced encryption capabilities that allow for processing of encrypted ciphers in a third-party environment while maintaining application functionality, Vaultive's platform supports the additional dimension of encryption of data in use. Vaultive's persistent encryption capabilities allow customers to satisfy requirements to encrypt data in transit to the cloud service provider, maintain encryption of data at rest while resident in the cloud, in addition to supporting encryption of data processed by a third-party service. This functionality set enables organizations to address their responsibility related to the custody of personal information as delineated under PIPEDA in two key aspects: firstly, by encrypting all personal information before it traverses a trusted boundary; and, by retaining the encryption keys to data resident on a third-party service, organizations can point to system controls to demonstrate fulfillment of the protection requirement.</td>
</tr>
</tbody>
</table>

---

1 Personal Information Protection and Electronic Documents Act, Current to September 4, 2012, CAN/CSA-Q830-96
| 4.7 Principle 7 – Safeguards | “The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.” | Vaultive’s platform addresses the requirements for security safeguards to protect against loss or theft of personal information through advanced encryption techniques that span the trusted network and the service provider’s environment. Based on the outcome of significant research and development in cryptography and key management, as well as ongoing product investments, the Vaultive platform maintains referential integrity to support processing of encrypted ciphers. Since the server-side processing is performed against encrypted data, data never resides in the clear outside of the trusted network. In addition, enterprise IT retains control of the encryption keys, providing an additional layer of controls to ensure protection of personal information and prevent unauthorized access. Because enterprise IT retains control of the encryption keys, disclosure requests from law enforcement agencies directed initially to the cloud service provider can be managed independently by the enterprise. Enterprise control of the encryption keys eliminates the risk that personal information can be inadvertently exposed to administrators at cloud service providers with access to customer instances. Were a hacker to be successful in their breach of the service provider’s environment, the data that they would retrieve from Vaultive’s customers would remain encrypted. The hacker would only gain access to the data or emails if they could also hack the encryption keys directly from the responsible organization. While cloud service providers would still be required to issue a notification should a breach take place, the use of Vaultive’s technology would reduce the scope of customer records that could be compromised, since they are in encrypted format. |
| 4.7 Principle 7 – Safeguards | “The methods of protection should include: (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and (c) technological measures, for example, the use of passwords and encryption.” | Vaultive’s enterprise-class cloud data encryption solutions enable customers to encrypt data-at-rest, data-in-transit and data-in-use in the cloud. Since enterprise cloud data is encrypted for the entire duration of its lifecycle (at-rest, in-transit and in-use), Vaultive’s market-leading capabilities for cloud data security serve to comprehensively insulate data from unauthorized access or targeted attacks by a third party. The Vaultive approach fully addresses the risk of inadvertent exposure of confidential data to administrators at the cloud service provider as enterprises reap the benefits from the moving their Exchange infrastructure to the cloud. Vaultive employs a patent-pending form of standard 256-bit AES encryption, supplemented with additional layer of encrypted metadata. In order to significantly minimize any statistical risk that the platform’s referential integrity for maintaining server-side processing of encrypted data can be compromised, Vaultive has invested heavily in several layers of compensating security measures. |
| 4.5 Principle 5 – Limiting use, disclosure, and retention: | “Organizations are required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records” | While service providers are compelled to comply with requests from law enforcement agencies delivered as a subpoena or a warrant to disclose personal information, once Vaultive is deployed only enterprise IT can release the keys to decrypt the data. This allows the organization to independently manage the government request. Additionally, the Vaultive appliance can be configured to ensure that data that moves beyond a specific jurisdictional domain remains encrypted. |
### CANADIAN PRIVACY AND DATA RESIDENCY REQUIREMENTS

<table>
<thead>
<tr>
<th>PIPA Requirement</th>
<th>Description of Controls</th>
<th>Vaultive Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasonable Technical Safeguards to protect personal information in their custody or control</td>
<td>Section 34 of the Personal Information Protection Act (&quot;PIPA&quot; or &quot;the Act&quot;) requires organizations “to protect personal information in their custody or control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.”</td>
<td>Vaultive's design goal is to deliver a platform that directly addresses the requirements for ownership and control of personal information under an organization's custody that resides or is processed on cloud-based services. Through deployment of the Vaultive proxy, organizations can encrypt data before it leaves the trusted network, while enterprise IT retains the encryption keys. Based on advanced encryption capabilities that allow for processing of encrypted ciphers in a third-party environment while maintaining application functionality, Vaultive's platform supports the additional dimension of encryption of data in use. vaultive's persistent encryption capabilities allow customers to satisfy requirements to encrypt data in transit to the cloud service provider, maintain encryption of data at rest while resident in the cloud, in addition to supporting encryption of data processed by a third-party service. This functionality set enables organizations to address their responsibility related to the custody of personal information as delineated under PIPA in two key aspects: firstly, by encrypting all personal information before it traverses a trusted boundary; and, by retaining the encryption keys to data resident on a third-party service, organizations can point to system level controls to demonstrate fulfillment of the protection requirement.</td>
</tr>
</tbody>
</table>

According to the Alberta Information and Privacy Commissioner’s report on privacy breaches in the province for the period of Jan 1- April 30 2012, of the 63 significant reported breaches, 14 were caused by electronic system compromises (with human error accounting for 22 of the total). These breaches were typically found to occur as a result of targeted attacks by external hackers seeking to extract large amounts of data. Were a hacker to be successful in their breach of the service provider’s environment, the data that they would retrieve from Vaultive’s customers would remain encrypted. The hacker would only gain access to the data or emails if they could also retrieve the encryption keys directly from the responsible organization.

---

2 Personal Information Protection Act, Province of Alberta, January 1, 2004
<table>
<thead>
<tr>
<th>PHIPA Requirement</th>
<th>Description of Controls</th>
<th>Vaultive Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practices to Protect Personal Health Information, Security</td>
<td>“A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.”</td>
<td>Vaultive’s persistent encryption capabilities allow customers to satisfy requirements to encrypt data in transit to the cloud service provider, maintain encryption of data at rest while resident in the cloud, in addition to supporting encryption of data processed by a third-party service. This functionality set enables organizations to address their responsibility related to the custody of personal information as delineated under PHIPA in two key aspects: firstly, by encrypting all personal information before it traverses a trusted boundary; and, by retaining the encryption keys to data resident on a third-party service, organizations can point to system level controls to demonstrate fulfillment of the protection requirement.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FIPPA (British Columbia Requirement)</th>
<th>Description of Controls</th>
<th>Vaultive Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of Privacy — Collection, Protection and Retention of Personal Information by Public Bodies</td>
<td>“A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.”</td>
<td>Vaultive’s persistent encryption capabilities allow customers to satisfy requirements to encrypt data in transit to the cloud service provider, maintain encryption of data at rest while resident in the cloud, in addition to supporting encryption of data processed by a third-party service. This functionality set enables organizations to address their responsibility related to the custody of personal information as delineated under FIPPA in two key aspects: firstly, by encrypting all personal information before it traverses a trusted boundary; and, by retaining the encryption keys to data resident on a third-party service, organizations can point to system level controls to demonstrate fulfillment of the protection requirement.</td>
</tr>
</tbody>
</table>

---

3 Personal Health Information Protection Act, Province of Ontario, January 1, 2004
4 Freedom of Information and Protection of Privacy Act, [Revised Statutes of British Columbia, 1996]
CANADIAN PRIVACY AND DATA RESIDENCY REQUIREMENTS

<table>
<thead>
<tr>
<th>FOIP Requirement</th>
<th>Description of Controls</th>
<th>Vaultive Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of Privacy — Collection, Protection and Retention of Personal Information by Public Bodies</td>
<td>“...reasonable security measures are followed to protect against unauthorized access, use, alteration, destruction, or disclosure of personal information.”</td>
<td>Vaultive’s persistent encryption capabilities allow customers to satisfy requirements to encrypt data in transit to the cloud service provider, maintain encryption of data at rest while resident in the cloud, in addition to supporting encryption of data processed by a third-party service. This functionality set enables organizations to address their responsibility related to the custody of personal information as delineated under FOIP in two crucial aspects: firstly, by encrypting all personal information before it traverses a trusted boundary; and, by retaining the encryption keys to data resident on a third-party service, organizations can point to system level controls to demonstrate fulfillment of the protection requirement.</td>
</tr>
</tbody>
</table>

Section II: Data Residency and Residency of Controls

Under Canadian privacy law, both federal bodies and commercial organizations domiciled within Canadian borders are responsible for the privacy and protection of personal information in their custody. This requirement applies regardless of where the data resides. While significant concerns have been articulated with regards to the probability of disclosure to US law enforcement agencies of data that resides within datacenters located within the US, the requirements pertain directly to the safeguards in place to maintain control.

As noted in her formal response to a question related to compliance with the Freedom of Information and Protection of Privacy Act presented by two members of the Ontario provincial parliament about the privacy and security of personal information collected by the Ministry of Natural Resources that is currently being stored in the U.S., Ann Cavoukian, Information and Privacy Commissioner for the Province of Ontario wrote:

“It is important to remember that, in Ontario, there is no legislative prohibition against the storing of personal information outside of the province or Canada. In other words, Ontario law, including the Act, does not speak to this issue. However, the Act and its regulations do require provincial institutions to ensure that reasonable measures are in place to protect the privacy and security of their records containing personal information. This applies regardless of where the records are located.”

5 The Freedom of Information and Protection of Privacy, Sec 38
Commissioner Cavoukian further added: “The critical question for institutions which have outsourced their operations across provincial or international borders is whether they have taken reasonable steps to protect the privacy and security of the records in their custody and control. I have always taken the position that you can outsource services, but you cannot outsource accountability.”

(Full document available at this link: [http://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf](http://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf))

The requirements, therefore, relate to where control of the data resides and the location of the data is not germane to the requirements.

**Vaultive Response: Maintaining Data Privacy and Control Residency**

Data residency and privacy challenges in the context of Canadian privacy compliance requirements pertain to limiting access to personal information in the custody of organizations subject to the legislation. Vaultive addresses this requirement to prevent unauthorized access by third parties through organizational control and ownership of the encryption keys and the application of persistent encryption.

Once encrypted at the boundary of the trusted network, the data remains encrypted, even when processed within the cloud service provider environment. Regardless of the jurisdiction where the data resides, control of the access to the data remains with the organization that retains the encryption key. For organizations that are hesitant about trans-border data flow, Vaultive’s persistent encryption ensures that data is never decrypted when resident in a third party’s environment.

![Figure 1: Vaultive Trans-Border Data Controls](image)

**Trans Border Data Controls**

Control of the keys in combination with Vaultive's encryption across the data lifecycle – in transit, at rest and in use – provide the foundation to satisfy requirements for control and adequate safeguards for the privacy of personal information.

---

**About Vaultive**

For businesses moving to the cloud, Vaultive's encryption in use technology mitigates risk by empowering companies with control and ownership of their data wherever it resides. Vaultive's customers hold the encryption keys, letting them retain the freedom to use the cloud applications professionals rely on, while ensuring the governance and security that the business demands. Optimized for multiple cloud applications, the Vaultive platform supports best practices for the control and ownership of corporate data in the cloud as outlined by the Cloud Security Alliance. Vaultive addresses the requirements of global enterprises in financial services, life sciences and pharma, legal and professional services, manufacturing, retail and media, while also offering a cost-effective solution for mid-size and smaller companies. For more information, visit [www.vaultive.com](http://www.vaultive.com) or follow us on Twitter [@vaultive](https://twitter.com/vaultive).