Cloud Computing Guide

Best Practices & Checklist

for Law Practices in Saskatchewan

NOVEMBER 2018

Law Society of Saskatchewan

Table of Contents

Overview 3
Background 3
Purpose 3
Audience 3
What is Cloud Computing and Cloud Services? 3
Definitions 4
Cloud Best Practices 5
Ensure Compliance with Privacy Acts 5
Canadian Privacy Laws 5
United States (US) Privacy Laws 7
European Union (EU) Privacy Laws 7
Understand and Manage your Client Data 8
Understand Cloud Security Risks 8
People 9
Process 10
Technology 10
Use Cloud Services Geographically Provided in Canada 11
Use Business, not Consumer Cloud Services 12
Regularly Review Cloud Service, Privacy Acts, & Client Data 12
Technology 12
Privacy Acts 13
Cloud Service Agreements 13
Client Data 13
Cloud Checklist 14
Cloud Data Privacy Compliance 14
Cloud Security & Risk 15
Cloud Technical Considerations 18
Law Society of Saskatchewan Considerations 19
Checklist Completion 20
Appendix A: Privacy Acts 21

Overview

Background

The use of cloud services through a cloud service provider has become pervasive. As personal use of cloud services has increased, the use of cloud services has also migrated into many businesses, including law practices.

Cloud services can provide several benefits to a law practice; such as, reduced capital and maintenance costs for IT equipment and software, and the introduction as a pay-as-you-go operating model for only those services consumed. However, moving to a cloud solution requires a law practice to consider factors such as privacy, security, regulatory compliance, and service availability.

There are continuous changes in cloud service terms and conditions, and modifications to jurisdictional regulations, that may affect how a law firm manages and retains data.

Purpose

The purpose of this document is to provide Saskatchewan law practices a set of best practices and a checklist to assist with evaluating cloud services. The information in this document should be used before selecting a cloud service provider or validating an existing cloud service provider.

Audience

The intended audience of this document are Saskatchewan based law practices where business is primarily conducted through a phone and laptop over the Internet. These law practices plan on utilizing the cloud with little to no internal IT support. While the law practice resides in Saskatchewan, clients may reside outside of the province or country.

While larger or inter-provincial law practices may take advantage of the information provided in this document, the document is not meant to be exhaustive as these law practices tend to have specific technical and regulatory requirements which cannot be addressed in a single document. It is advisable for larger law practices to engage professional IT services that can provide consultation based on the practice's specific requirements.

What is Cloud Computing and Cloud Services?

In the simplest terms *cloud computing*[1] *means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet.*

Below are some examples and definitions of cloud services widely used today:

Social Networking – Facebook, LinkedIn, Twitter, etc. The main idea of social networking is to find people someone may already know or people someone would like to know and share information with them.

[1] What is Cloud Computing: https://www.pcmag.com/article2/0,2817,2372163,00.asp

Email – Outlook.com, Gmail, etc. Web-based email service hosted from a cloud service provider that can be accessed from anywhere.

Document Hosting – Microsoft Office 365, Google Docs, etc. Web-based hosting of document creation and management solutions that allow for easy collaboration among multiple contributors.

File Sharing and Data Storage – One Drive, Box, Dropbox, etc. Cloud-based services that allows for the storage of a variety of file types (documents, pictures, videos, etc.), accessible from multiple platforms (phone, computer, tablet, etc.), from anywhere in the world, and shareable with friends and peers.

Definitions

Term	Definition
Antivirus/Anti-malware	A type of utility used for scanning and removing viruses from your computer. While many types of antivirus (or "anti-virus") programs exist, their primary purpose is to protect computers from viruses and remove any viruses that are found.
Cloud Computing	A shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, like a public utility.
Cloud Service Provider (CSP)	Cloud service providers (CSP) are companies that offer network services, infrastructure, or business applications in the cloud. The cloud services are hosted in a data center that can be accessed by companies or individuals using network connectivity.
Cloud Service	A cloud service is any service made available to users on demand via the Internet from a cloud computing provider (CSP) as opposed to being provided from a company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by a cloud services provider.
Data Centre	A central location for computer network hardware and software, especially storage devices for data.
Encryption	A method of putting information in code so that only authorized users will be able to see or use the information.
FISA	Foreign Intelligence Surveillance Act
GDPR	General Data Protection Regulation
Malware	Software programs designed to damage or do other unwanted actions on a computer system.
Network	A group of computers that communicate with each other.
PIPEDA	The Personal Information Protection and Electronic Documents Act
Safe-harboured	Having a copy of your data stored securely by a 3rd provider separate from the cloud provider to guard against data loss and/or the cloud provider ceasing business.
Server	A computer that hosts systems or data for use by other computers on a network.

USA FREEDOM Act	Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
Virus	Computer viruses are small programs or scripts that can negatively affect the health of your computer.
Virtual Private Network (VPN)	Extends a private network across the internet and enables users to send and receive data as if their laptop or phone were directly connected to the cloud provider or service. The data is also encrypted during transmission over the network.

Cloud Best Practices

Ensure Compliance with Privacy Acts

There are one or more privacy acts that will affect Saskatchewan law practices. These privacy acts are created and managed by various regulatory bodies provincially, nationally, and internationally.

Each law practice will have a unique list of privacy acts and associated regulation that require compliance due to factors like geographical location of the client, geographical location of where the cloud service is hosted and the type of law practice client (e.g. private, public, etc.).

As such, each law practice will need to determine what privacy acts and associated regulations will require compliance and then ensure compliance is met. The following question can assist with determining which privacy acts require compliance:

- What is the geographical location of the law practice and/or employees?
- What is the geographical location of the law practice client?
- Where geographical location is the cloud service being provided (Canada, US, International)?
- Does the data cross provincial or national borders?
- Is the law practice client private, public, or a non-for-profit?

Canadian Privacy Laws

There are several laws in Canada that relate to privacy rights. Enforcement of these laws is handled by various government organizations and agencies. The Office of the Privacy Commissioner of Canada has provided information that can assist with determining which Canadian privacy acts require compliance: Summary of privacy laws in Canada[2]. This information needs to be reviewed and validated for compliance.

For private-sector, for-profit entities every Saskatchewan law practice needs to know and ensure compliance with Canada's privacy act PIPEDA[3,4]. An organization is responsible for the protection and fair handling of personal information at all times. This applies throughout its organization and in dealings with third parties.

[2] Summary of privacy laws in Canada: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/
[3] The Personal Information Protection and Electronic Documents Act (PIPEDA): https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2-2
[4] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5): https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

PIPEDA[3,4] sets the ground rules for how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities across Canada. It also applies to the personal information of employees of federally-regulated businesses such as banks, airlines, and telecommunications companies.

PIPEDA[3,4] does not apply to organizations that do not engage in commercial, for-profit activities such as charities and political parties. Municipalities, universities, schools, and hospitals (MUSH-sector[5]) are generally covered by provincial law, PIPEDA[3,4] may only apply in certain situations.

Every province and territory have its own laws that apply to provincial government agencies and their handling of personal information. Alberta, British Columbia, and Quebec have private-sector privacy laws that have been deemed "substantially similar"[6] to PIPEDA[3,4] which means that those laws apply instead of PIPEDA[3,4] in some cases. Saskatchewan does not have its own private-sector privacy laws so PIPEDA[3,4] applies.

PIPEDA[3,4] has a set of principles referred to as the Fair Information Principles[7] . As these principles are the foundation of PIPEDA and will have associated regulation that require compliance:

Principle 1 - Accountability: An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.
Principle 2 - Identifying Purposes: The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.
Principle 3 - Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate[8].
Principle 4 - Limiting Collection: The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.
Principle 5 - Limiting Use, Disclosure, and Retention: Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.
Principle 6 - Accuracy: Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.
Principle 7 - Safeguards: Personal information must be protected by appropriate security relative to the sensitivity of the information.
Principle 8 - Openness: An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.
Principle 9 - Individual Access: Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual

[5] The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/
[6] Provincial legislation deemed substantially similar to PIPEDA: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/
[7] PIPEDA fair information principles: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/
[8] Applying paragraphs 7(3)(d.1) and 7(3)(d.2) of PIPEDA: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/gd_d1-d2_201703/

shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 - Challenging Compliance: An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA[3,4], usually their Chief Privacy Officer.

United States (US) Privacy Laws

There is no centralized federal privacy law or legislation in the US regulation the collection and use of personal data. In the US, data privacy is based on a system of federal and state laws that can overlap and even contradict each other. Federal privacy-related laws are typically categorized in sectors such as financial, health, or electronic communications.

For a Saskatchewan law practice, if data is transferred or is stored with a cloud service provider geographically located within the US, the predominant acts that require understanding and compliance are:

- **FISA**[9] - Foreign Intelligence Surveillance Act
- **USA PATRIOT Act**[10,11] - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
- **USA FREEDOM Act**[12] - Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act

Under these three acts, the US government can legally look at an individual's data that is held by a third party without notice to the owner of the data. These searches can be physical searches and/or telecommunication surveillance which includes wiretapping phones, accessing voicemail, intercepting email and text messages and wiretapping VoIP calls. The FBI can force cloud service providers to provide client data.

European Union (EU) Privacy Laws

The European Union (EU) has a comprehensive set of personal data protections in the form of a regulation called the General Data Protection Regulation (GDPR)[13] within EU law. GDPR[13] aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business (including Canada) by unifying the regulation within the EU.

GDPR[13] contains provisions and requirements pertaining any client that may reside in the EU or any cloud data provider that may provide cloud services geographically within the EU. GDPR[13] also addresses the export of personal data outside the EU and European Economic Area (EEA)14 areas.

Saskatchewan law practices that handle personal data from any client geographically located in the EU must provide safeguards to protect client data so the client data is not available publicly without explicit, informed consent. The personal client data cannot be used to identify a client without additional information stored separately. No personal client data may be used in the cloud unless it is done under a lawful basis specified by

---

[9] FISA Description: https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act
[10] USA Patriot Act Description: https://en.wikipedia.org/wiki/Patriot_Act
[11] USA Patriot Act Website: https://www.justice.gov/archive/ll/highlights.htm
[12] USA Freedom Act Description: https://en.wikipedia.org/wiki/USA_Freedom_Act
[13] General Data Protection Regulation (GDPR): https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
[14] EEA Description: https://en.wikipedia.org/wiki/European_Economic_Area

the regulation or unless the law practice has received consent from the client related to the data. The client has the right to revoke this consent at any time.

Understand and Manage your Client Data

To successfully address client data privacy regulations and protect client data in the cloud, a law practice needs to know and understand what data is stored, what data is sensitive, and when the data requires client permission to retain or be removed. Client data needs to be identified and managed based on the regulatory acts related to the client. For example, in PIPEDA[3,4] client permission is required if their data is retained and used for purposes other than those originally intended. If permission is not sought after or client permission has not been granted, the client data may need to be removed from the cloud service.

Client data identified as sensitive needs to be managed according to the applicable privacy act and regulation. For example, PIPEDA[3,4] lists the following types of data as sensitive:

- race, national or ethnic origin
- religion
- age, marital status
- medical, education or employment history
- financial information
- DNA
- identifying numbers such as social insurance number, or driver's licence
- views or opinions about employees

Client information could be used to determine their behaviours and preferences which can be a wealth of information that others can use to fuel analytics for insight and gain. For example, some cloud service providers provide consumer email services that collect that personal information, then aggregate that data and resell to others for profit. As a steward of client data, a law practice needs to ensure their client data is not shared with others without their client's consent.

Privacy and data usage for a law practice can reflect culture and values. Client data privacy can be a competitive differentiator, especially if other law practices are not following good practices or worse, penalized for failing to meet regulatory compliance.

Law practices also need to consider the impact of consumer expectations as well as individual interpretations of privacy. What's acceptable to one client not be acceptable to another, regardless of specific regulatory requirements.

Managing client data through discovery and classification, and then protection and monitoring can be significant challenge for a law practice as it can be laborious and time consuming. Some cloud service providers are now supplying technology to assist with data privacy management to ease the burden.

Understand Cloud Security Risks

While closely related, security and privacy are not interchangeable. Data can be highly secured while violating a client's privacy. For example, data may be encrypted end to end, but the data is not being used for its original purpose without the consent of the client.

The introduction of cloud services can introduce or amplify existing security issues. Although shifting to cloud technologies exclusively may provide cost and efficiency gains, doing so requires that business-level security

policies, processes, and best practices be considered. The absence of good cloud security can make a law practice vulnerable to security risks that can erase any gains made by the switch to cloud technology.

The Cloud Security Alliance Group has documented a number of cloud service threats "The Treacherous 12 - Cloud Computing Top Threats in 2016"[15] that need to be understood and considered as risks:

1. **Data Breaches –** sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so.
2. **Weak Identity, Credential and Access Management –** lack of identity access, failure to use multifactor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates.
3. **Insecure Application Programming Interfaces (APIs) –** accidental and malicious attempts to circumvent policy using authentication, access control, encryption and activity monitoring.
4. **System and Application Vulnerabilities –** exploitable bugs in programs that attackers can use to infiltrate a cloud service for stealing data, taking control of the cloud service or disrupting cloud service operations.
5. **Account Hijacking –** attack methods such as phishing, fraud and exploitation of cloud service vulnerabilities.
6. **Malicious Insiders –** a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or cloud service
7. **Advanced Persistent Threats (APTs) –** parasitical form of cyberattack that infiltrates systems to establish a foothold in a cloud service of target companies and then smuggling data and intellectual property. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them.
8. **Data Loss –** intentional or accidental loss of data. The burden of avoiding data loss does not solely fall on the cloud service provider but also the cloud service customer.
9. **Insufficient Due Diligence** - a rush to adopt cloud services without performing due diligence exposes a myriad of commercial, financial, technical, legal and compliance risks.
10. **Abuse and Nefarious Use of Cloud Services –** misuse of cloud service-based resources include launching DoS[16] attacks, email spam and phishing campaigns; "mining" for digital currency; large-scale automated click fraud; brute-force compute attacks of stolen credential databases; and hosting of malicious or pirated content.
11. **Denial of Service (DoS)[16] –** attacks meant to prevent users of a cloud service from being able to access their data or cloud services by forcing the targeted cloud service to consume inordinate amounts of finite system resources.
12. **Shared Technology Issues –** sharing infrastructure, platforms or applications. Underlying cloud services components multi-customer applications leading to shared technology vulnerabilities that can potentially be exploited.

Cloud services security and risk mitigation requires a combination of *people*, *process*, and *technology* with all three aligned:

People

[15] The Treacherous 12: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
[16] Denial of Service (DoS) definition: https://en.wikipedia.org/wiki/Denial-of-service_attack

A highly secure cloud service can still be exploited through inappropriate use or management of a cloud service. Inappropriate use or management of cloud services can be unintentional as security risks may not be obvious.

Every user of a cloud service needs to know and understand potential security risk types as well as how to avoid, mitigate and respond to a security event should a response be required. It is advisable for a law practice to establish training on potential security risks, security responses and good data management. As well, training should be provided on how to securely use technologies that do not increase the change of someone gaining access to a law practices cloud services or data (e.g. phishing[17], social engineering[18], etc.)

Process

A series of repeatable processes should be documented and established as standard policies within a law practice. The policies should be documented in a way that can be clearly communicated to others within the law practice as well as clients who are trusting their data is secure.

Good security processes and policies can be enforced by having good cloud security controls[19]. The following security controls should have policies and processes documented for each:

1. **Deterrent –** intended to reduce attacks on a cloud service. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed.
2. **Preventive –** strengthen the cloud service against security incidents by reducing vulnerabilities.
3. **Detective –** detect and react appropriately to security incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.
4. **Corrective –** reduce the consequences of an incident, normally by limiting the damage which come into effect during or after an incident.

Technology

There are a number of technologies that should be used to deter, prevent, detect and correct risks and security threats; these technologies also support connecting to and using the cloud service through a device such as a laptop or phone and over the internet. Some cloud service providers implicitly provide security-based technologies as part of their service.

Each law practice will have different technology requirements based on factors such as their size and the sensitivity of the data they responsible for. As such, each law practice will need to identify and deploy technology that is right for them that matches the appropriate security threat level.

While technology requirements can be unique for each law practice, the following list of technologies is recommended at a minimum:

Laptop/Smart Phone

[17] Phishing Definition: https://en.wikipedia.org/wiki/Phishing
[18] Social Engineering Definition: https://en.wikipedia.org/wiki/Social_engineering_(security)
[19] Cloud Computing Security: https://en.wikipedia.org/wiki/Cloud_computing_security

1. **Antivirus/Anti-malware**[20] **–** designed to protect computers against viruses and malware[21] such as spyware[22], adware[23], and rootkits[24].
2. **Local disk (storage) Encryption**[25] **–** protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people.

Internet Connection

1. **Virtual Private Network (VPN)**[26] **-** extends a private network across the internet and enables users to send and receive data as if their laptop or phone were directly connected to the cloud provider or service. The data is also encrypted during transmission over the network.
2. **Wireless Intrusion Prevention System (wIPS)**[27] **–** on a wireless network, monitors for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures.

Cloud Service

1. **Encryption**[28] **(in transit, at rest) –** protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people.
2. **Two-Factor Authentication (2FA)**[29] **–** a method of confirming users' claimed identities by using a combination of two different factors: something they know, something they have, or something they are.
3. **Security & Incident Detection, Alerting and Logging –** proactively detect and alert on areas of high risk, keep history of events for compliance.

Use Cloud Services Geographically Provided in Canada

While it is possible to use cloud services provided from areas outside of Canada, it is advisable not to. The law practice is accountable for all client data including data that is transferred and placed with a cloud service provider.

Data transmitted and/or stored outside of Canada can be subject to another jurisdiction's laws or regulations. For example, the USA Patriot Act permits US law enforcement agencies to require US entities to supply a client's data if ordered. The order for data can apply to information that is geographically located in the US, Canada, or elsewhere. US cloud service providers can be ordered to provide information that exists in Canada or the US. The US cloud service provider is subject is not permitted to reveal the existence of the order request or that it provided information.

As part of PIPEDA[3,4] data transfer rules, if a client's data is to be transmitted or stored outside of Canada, the client needs to be informed, be educated on the risks, and approve of:

---

[20] Antivirus Definition: https://techterms.com/definition/antivirus
[21] Malware Definition: https://techterms.com/definition/malware
[22] Spyware Definition: https://techterms.com/definition/spyware
[23] Adware Definition: https://techterms.com/definition/adware
[24] Rootkit Definition: https://techterms.com/definition/rootkit
[25] Disk Encryption Definition: https://en.wikipedia.org/wiki/Disk_encryption
[26] Virtual Private Network Definition: https://en.wikipedia.org/wiki/Virtual_private_network
[27] wIPS Definition: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system
[28] Encryption Definition: https://techterms.com/definition/encryption
[29] Multi-factor authentication Definition: https://en.wikipedia.org/wiki/Multi-factor_authentication

- their personal information being transferred outside of Canada for processing and/or storage.
- their personal information being subject to the laws of the foreign jurisdiction including their personal data could be taken and read by foreign governments.

Informing and seeking approval from each client could be laborious and time-consuming. There is also a risk that a client may choose to not allow their data to leave Canada resulting in another cloud service solution being required.

Canadian cloud providers have the best knowledge of the country's privacy laws and are in the best position to securely store client data. Keeping data geographically located in Canada is much simpler, requires less privacy compliance and has a reduced risk of being anonymously provided from other jurisdictions.

Use Business, not Consumer Cloud Services

Cloud computing has become pervasive with the advent of cloud services like Facebook, Dropbox, Instagram, Twitter, etc. typically, not being charged a fee for the use of the service and that cloud services ease-of-use. As the cloud service provider is not directly charging a fee for the use of the cloud service, the cloud service provider earns revenue from advertising and consumer data collection.

Business cloud service providers typically charge for the use of their business cloud service which is billed directly rather than advertising or data collection. Business cloud services are also typically purpose-built for availability, data privacy and security while also providing additional service options that are not present in consumer cloud services.

Some cloud service providers offer solutions like email, word processing, spreadsheets, and online file storage at no direct cost to the user. Due to the low cost and ease-of-use, it can be tempting to use consumer cloud services for business use. Unfortunately, there is a high likelihood that a law practice putting client data on a consumer client service has a higher risk of exposing the data to others and not meeting regulatory requirements.

Regularly Review Cloud Service, Privacy Acts, & Client Data

Cloud technology as well as privacy regulations are constantly changing and evolving. Understanding what has changed can be a challenge, especially if the benefits of a cloud service is already being realized. With any change, risks from change need to be identified and actioned.

It is recommended to set up an annual process that ensures there is a regular review of cloud service technology, the client data that is already stored on that cloud service, and a review of new and existing privacy acts.

Technology

Technology changes very rapidly. Cloud services have brought about a significant change in how people and organizations view and use technology. As well, the devices that are used to consume cloud services have evolved and changed. For example, the use of smart phones is pervasive today and has surpassed the use of computers and laptop for daily use.

Existing technology needs to be reviewed to ensure it still meets the security and regulatory requirements. As well, cloud service providers are regularly adding or updating technical capabilities and locations that could improve security, auditing, and compliance.

Privacy Acts

Increased privacy regulation has been rapidly introduced over the past decade. Existing regulation is under constant change as they are challenged, and regulators respond to privacy and security events. Regulations created in another jurisdiction may be assumed to only affect that jurisdiction, unfortunately that may not be the case. For example, GDPR[13] was recently introduced in Europe. While in theory, GDPR[13] applies to EU citizen data, it is possible that non-EU entities could also be affected.

Cloud Service Agreements

Cloud service providers are continually updating their Service Level Agreements (SLA). Many changes to made to SLA's are based on the cloud service provider responding to changes in regulation or changes to how the cloud service providers wishes to provide service their customers.

Any change to an SLA needs to be reviewed to ensure the cloud service is delivered intended, does not change client data ownership rules, and does not violate privacy acts.

Client Data

A law practice needs to ensure that any stored client data meets regulatory compliance such as PIPEDA[3,4], GDPR[13], etc. Between changes to regulations and changes to client data, a regular review of client data will ensure compliance as well as client trust with their data.

Meeting regulatory compliance means a law practice must actively manage their client data. Client data cannot be created and forgotten.

Cloud Checklist

Cloud Data Privacy Compliance

	Yes	No
1. Have you read the following privacy acts?		
a. PIPEDA[3,4]	☐	☐
b. FISA[9]/USA PATRIOT Act[10,11]/USA FREEDOM Act[12]	☐	☐
c. GDPR[13]	☐	☐
d. Other	☐	☐
2. Do you have clients in the following geographical locations?		
a. Saskatchewan	☐	☐
b. Canada	☐	☐
c. United States	☐	☐
d. European Union (EU)	☐	☐
e. Other	☐	☐
2. Do you have cloud services being provided from the following geographical locations?		
a. Canada	☐	☐
b. United States	☐	☐
c. European Union (EU)	☐	☐
d. Other	☐	☐
3. Have you identified what privacy acts regulate client data based on the client's geographical location (e.g. PIPEDA[3,4], GDPR[13], etc.)?	☐	☐
4. Have you identified what privacy acts regulate client data based on geographical location of where the cloud service is hosted (e.g. PIPEDA[3,4], GDPR[13], etc.)?	☐	☐
5. Have you identified what privacy acts regulate client data based on geographical location of where the cloud service is hosted (e.g. PIPEDA[3,4], GDPR[13], etc.)?	☐	☐
6. Have you reviewed and categorized personal or sensitive client data as required by the identified privacy acts?	☐	☐

7. Does your law practice have a process to change or remove client data to meet compliance requirements if required?	☐	☐
8. Does all your client data meet regulatory compliance requirements for the identified regulatory acts?	☐	☐
a. Do you have the client's permission to retain their data for its original purpose?	☐	☐
b. Have you acquired client consent if client data is to be retained after its original purpose?	☐	☐
c. Do you have client consent if their data is being disclosed for a secondary purpose?	☐	☐
9. Do you have any data being transmitted outside of Canada?	☐	☐
a. If so, has the client been informed?	☐	☐
b. If so, have you received consent from the client?	☐	☐
10. Does your cloud service provider have any language, guarantees or representations regarding the security or integrity of your client's data based on the identified regulatory acts?	☐	☐
11. Does your law practice have a data privacy policy that discloses how client data is and/or will be used, managed, and shared?	☐	☐
a. If so, has your law practice communicated the data privacy policy to clients?	☐	☐
b. If so, has your law practice confirmed all cloud services are or will consistent with the law practices data privacy policy?	☐	☐
12. Does the cloud service provider share all or parts your client's cloud data to other parties?	☐	☐
a. If so, do you have permission from the client to share cloud data with the cloud service provider?	☐	☐
b. If so, does your cloud service provider have client permission to share your cloud data with other parties?	☐	☐

Cloud Security & Risk

	Yes	No
1. Can your law practice operate if the cloud service is unavailable?	☐	☐
a. Do you have documented manual processes in place to operate your law practice while the cloud service is unavailable?	☐	☐
2. Have you read the cloud provider's 'click-thru' agreement?	☐	☐
3. Have you read the cloud provider's SLA (Service Level Agreement)?	☐	☐

	Yes	No
4. Does the SLA ensure intellectual property rights and/or ownership rights to your data are not transferred during the life of the contract as well as after?	☐	☐
5. Will the cloud service provider give your firm notice when the SLA agreement and other underlying policies are changed?	☐	☐
6. Is there a dispute resolution method or process in the cloud provider's SLA?	☐	☐
7. Have you read the cloud service provider's Privacy and Confidentiality Agreement?	☐	☐
8. Will your cloud provider notify you of security breaches that could affect your data?	☐	☐
9. Does your cloud service provider have a means to monitor for and report abuse of the cloud service (e.g. Denial-of-Service attacks)?	☐	☐
a. Do you audit the cloud provider's data security performance?	☐	☐
b. Does your law practice have a documented process to follow if a security or privacy breach occurs?	☐	☐
10. Does your cloud provider have a policy and process to handle ransomware attacks?	☐	☐
a. Does your cloud provider carry liability insurance associated with ransomware attacks?	☐	☐
b. Can your cloud provider recover your data in the event your data and/or cloud service is no longer available to you?	☐	☐
11. Does your law practice have a policy and process to handle ransomware attacks?	☐	☐
a. Can your cloud provider or you recover your data in the event your data and/or cloud service is no longer available to you?	☐	☐
b. Does your law practice carry liability insurance associated with ransomware attacks?	☐	☐
c. In the event your data is locked or taken, do you know who you communicate to and how you would respond to clients and regulators?		
12. Is your cloud service provider able to retain and/or archive required data for the legally specified period (e.g. law practice accounting information)?	☐	☐
13. Do you or your cloud service provider have a disaster recovery/business continuity plan?	☐	☐
a. Are backups stored in a safe, secure and fireproof location?	☐	☐
i. Local backup?	☐	☐
ii. 3rd party (cloud-based) backup provider?	☐	☐
b. Can you recover your cloud data and/or cloud service from backup in the event of a data breach, the cloud provider losses your data or no longer provides cloud services to you?	☐	☐

	Yes	No
14. Do you have a documented cloud exit strategy in the event you wish to move away from a cloud provider?	☐	☐
a. Can your data be easily moved from one cloud provider to another?	☐	☐
b. Will the cloud service provider provide your data in a format that can be moved to another cloud provider?	☐	☐
c. Will the cloud provider retain your data for an extended period of time in the event your contract with the cloud provider ends?	☐	☐
d. Do you know the length of time it would take to migrate data from one cloud service provider to another and is that time acceptable?	☐	☐
15. Is the cloud provider required to compensate you for losses as a result of using their service?	☐	☐
a. Do you have third-party insurance to cover this?	☐	☐
b. Have you ensured there is no cap on the cloud provider's liability?	☐	☐
c. Can you terminate the cloud service without penalty?	☐	☐
d. Is the cloud provider required to provide transition support if the service is terminated?	☐	☐
e. Can your data be sanitized from the cloud provider in the event of a termination?	☐	☐
16. Does the cloud service provider use other 3rd party cloud services ('clouds of clouds')?	☐	☐
a. If so, is the location of the 3rd party cloud service provider within Canada?	☐	☐
b. If so, does the 3rd party cloud service provider fall under the original cloud services contractual terms and conditions?	☐	☐
c. If so, does the 3rd party cloud service provider meet the identified regulatory requirements?	☐	☐
d. If so, Is the cloud service provider required to give notice if contemplating contracting out to other providers?	☐	☐
e. If so, has your clients been informed of the geographical location of their data, what data is being use/stored, and their options to opt out?	☐	☐
17. Does the cloud service provider use a sub-contractor?	☐	☐
a. If so, is the location of the sub-contractor within Canada?	☐	☐
b. If so, does the sub-contractor fall under the original cloud services contractual terms and conditions?	☐	☐

	Yes	No
c. If so, does the sub-contractor meet the identified regulatory requirements?	☐	☐
d. If so, Is the cloud service provider required to give notice if contemplating contracting out to sub-contractors?	☐	☐
e. If so, has your clients been informed of the use of sub-contractors and their options to opt out of the cloud service?	☐	☐

Cloud Technical Considerations

	Yes	No
1. Do you have a requirement to integrate a cloud service with another cloud service or internal office system?	☐	☐
a. If so, does the cloud service integrate with your other office systems including other cloud services if required?	☐	☐
b. Do you know the level of IT support that will be required to support the cloud service integration?	☐	☐
2. Is the cloud service meet your requirements for availability?	☐	☐
a. Is there an extra cost to ensure the cloud service availability?	☐	☐
b. Have you checked your cloud providers actual availability history to ensure it meets your availability requirements?	☐	☐
3. Do you encrypt your data?		
a. On a client device (phone, laptop, etc.)?	☐	☐
b. In motion over the Internet (e.g. VPN)?	☐	☐
c. On the cloud? (often called data at rest)	☐	☐
4. Do you have sufficient Internet bandwidth to run the cloud application with acceptable performance?	☐	☐
5. Do you have a secondary internet connect should the primary internet connection not be available? (e.g. Cellphone as a wireless hotspot)	☐	☐
6. Can the cloud service scale (increase or decrease) based on demand?	☐	☐
7. Does the cloud service provider have multiple types of security?		
a. Company-based security (intrusion detection and prevention, spam and virus filters, etc.)	☐	☐
b. Access based security (based on identity or role of an individual in your organization)	☐	☐

	Yes	No
c. Transport-based security (such as Virtual Private Network or VPN, Secure Socket Layer or SSL tunneling or encryption)	☐	☐
d. Multi-Factor/Two-Factor Authentication	☐	☐
8. Is there an extensive knowledge base on the cloud service for self-help and support?	☐	☐
9. Cloud provider direct support:		
a. Do the times of available support match your typical operating hours?	☐	☐
b. Is there emergency contact information?	☐	☐
c. Does the method of communication (phone, email, text) match your requirements?	☐	☐
10. Does your cloud provider meet backup and recovery requirements for:		
a. Immediate data recovery with no data loss?	☐	☐
b. Data Archiving?	☐	☐
c. Disaster Recovery?	☐	☐
11. Are availability, performance and bandwidth representations spelled out in the SLA?	☐	☐
a. Are there penalties for your cloud provider not meeting their SLA's?	☐	☐
12. Does your cloud service provider require planned outages for maintenance?	☐	☐
a. If so, will you be given adequate notice for maintenance periods?	☐	☐
b. Are the cloud provider's schedule and duration for maintenance acceptable?	☐	☐
c. Does your cloud provider need you to test the cloud service before, during, or after the maintenance period?	☐	☐

Law Society of Saskatchewan Considerations

	Yes	No
1. Can you print (or convert to PDF) the following electronic records monthly?		
a. trust journal	☐	☐
b. trust reconciliation including client trust listing	☐	☐
c. trust property record	☐	☐

	Yes	No
2. Can electronic records be printed (or converted to PDF) on demand?		
a. client trust ledger cards monthly	☐	☐
b. client trust at the conclusion of the matter	☐	☐
c. general journal	☐	☐
d. general bank reconciliation	☐	☐
e. billing journal	☐	☐
f. accounts receivable detail and listings	☐	☐
g. billings for all fees, charges and disbursements in chronological or numerical order	☐	☐
3. Do you maintain a hard copy or PDF of the master billings file ?	☐	☐
4. Do you print or PDF all accounting records on an ongoing basis and store them appropriately?	☐	☐
5. Do your trust account reconciliations show the date that the reconciliation was completed?	☐	☐
a. Is an acceptable audit trail available on demand in a comprehensible format (print or PDF)?	☐	☐
6. Are all your cash receipts retained in hard copy form?	☐	☐
7. For all records, does the system record the creation and change dates?	☐	☐
a. Does the system preserve all metadata regarding electronic documents?	☐	☐
8. Have you considered your professional obligations that arise when you lose custody or control of your or your client's data?	☐	☐
9. Your electronic records must be capable of meeting the prevailing electronic discovery standards of the Courts. Have you verified this?	☐	☐

Checklist Completion

	Yes	No
1. Have you setup a re-occurring process that ensures your law practice reviews:		
a. This document for revisions and changes?	☐	☐
b. For new regulatory acts that have been created?	☐	☐

c. Existing regulatory acts for changes in language?	☐	☐
d. Changes to the cloud services technology and/or how the cloud service is delivered which could affect security or regulation?	☐	☐
e. Cloud service providers agreements for compliance with regulations?	☐	☐
2. Have you fully completed this checklist and recorded the information for later reference?	☐	☐

Appendix A: Privacy Acts

Region	Regulator/Act	Sector	Supporting Information
Saskatchewan	The Freedom of Information and Protection of Privacy Act (FOIP)	Saskatchewan Public Sector	https://oipc.sk.ca/ http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf
	The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)	Saskatchewan Public Sector	https://oipc.sk.ca/ http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/L27-1.pdf
	The Health Information Protection Act (HIPA)	Saskatchewan Public Sector	https://oipc.sk.ca/ http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0-021.pdf
Canada	The Privacy Act	Canada Federal Government	http://laws-lois.justice.gc.ca/eng/acts/P-21/page-11.html#h-35
	Personal Information Protection and Electronic Documents Act (PIPEDA)	Canada Private Sector	https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/
Alberta	Personal Information Protection Act (PIPA)	Alberta Private Sector	http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779762507
	Freedom of Information and Protection of Privacy Act	Alberta Public Sector	http://www.servicealberta.ca/foip/
British Columbia	Personal Information Protection Act	British Columbia	http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01
Quebec	Act respecting the protection of personal information in the private sector	Quebec Private Sector	http://legisquebec.gouv.qc.ca/en/ShowDoc/cs/P-39.1/
USA	Patriot Act	Public or Private Sector, Any	https://www.justice.gov/archive/ll/highlights.htm
	Federal Trade Commission Act	Companies and individuals doing business in the US	https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act

Region	Regulator/Act	Sector	Supporting Information
	Financial Services Modernization Act	Companies and individuals doing business in the US	https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act
	Health Insurance Portability and Accountability Act (HIPAA)	Companies and individuals doing business in the US	https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
	Electronic Communications Privacy Act	Companies and individuals doing business in the US	https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285
	Federal Trade Commission (FTC)	Companies and individuals doing business in the US	https://www.ftc.gov/
	Others	All	https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1
European Union (EU)	General Data Protection Regulation (GDPR) [13]	All	https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49751