Deloitte.

Data privacy in the cloud
Navigating the new privacy regime in a cloud environment

The era of the cloud is here! It is a game-changing innovation that includes a broad set of public, private, and business process outsourcing capabilities. Cloud-based services offer unparalleled scalability, elasticity, and flexibility. The business benefits are so compelling that adoption is likely to continue growing at a rapid pace across all industries and sectors.

By 2020, a no-cloud policy will be as rare as a no-internet policy is today.

Predicts 2016: Cloud Computing to Drive Digital Business (Gartner)

Today, the cloud offers flexible and affordable software, platforms, infrastructure, and storage available to organizations across all industries. Faced with limited budgets and increasing growth demands, cloud computing presents an opportunity for organizations to reduce costs, increase flexibility, and improve IT capability.

Types of cloud services

Private cloud
Tools that provide scalability and self-service on proprietary architecture

Infrastructure as a service
On-demand and scalable compute, storage, and networking hosted by a provider

Platform as a service
Collection of tools needed for application development hosted by a provider

Software as a service
Applications hosted by a provider and consumed by customers over the internet

Personal cloud
Provider-hosted capabilities from storage, to media streaming, to collaboration, accessible through personal accounts

Cloud services globally will reach $312 billion annually by 2019, with year-over-year growth of over 15 percent.[1] In fact, cloud services will be the fastest growing segment of IT spending as a whole as organizations begin to take advantage of the high degree of standardization, self-service functionality, and level of automation offered by paying only for what they need when they need it.[2]

However, the adoption of cloud computing raises challenges in the face of new, and often competing, privacy regulations across various jurisdictions, as well as evolving cybersecurity threats. For example, organizations that rely on multiple cloud service providers may have little or no control over the movement of their data through different data centres around the world. Similarly, it is not always clear whether the data custodian or the third-party service provider is accountable to protect the data, or which sets of data protection laws apply. Moreover, cloud service providers are often reluctant to fully disclose the security measures they use to protect information or how they process the data, which is problematic in light of the proliferation and magnitude of recent privacy breaches resulting in privacy class action lawsuits and reputational damage for cloud system users.

As a result, it is not surprising that organizations moving to the next generation of outsourced cloud services are concerned about privacy and data protection in the cloud.

[1] Gartner (2015, August 26) Forecast Analysis: Public Cloud Services, Worldwide, 2Q15 Update
[2] Forrester (2015, December 8) TechRadar Cloud Computing Q4 2015

Key considerations

There is no single answer to the regulatory, privacy, and security challenges raised by cloud computing, but here are three important steps you can take to protect your data in the cloud:

Understand and comply with various jurisdictional privacy laws.

You can only understand your risks and obligations when you are aware of the legal requirements of the local jurisdiction where the data originates and where it ends up being stored or processed.

Understand how your cloud provider will protect your data.

The legal trend is disrupting the supply chain of cloud computing by making everyone accountable for data privacy, not just the data custodian/controller.

Explore different encryption technologies and tools.

The market continues to see a wide variety of tools and capabilities offered, which provide mechanisms for encrypting, anonymizing, and otherwise securing your information.

Step 1:
Where is your data stored?
Understand and comply with various jurisdictional privacy laws

Under cloud computing models, data is often processed or stored in multiple jurisdictions, creating overlapping jurisdictions for Canadian-domiciled organizations and multinationals. This means these organizations are responsible for complying with Canadian privacy laws, as well as the privacy laws in other jurisdictions.

Canadian laws

In Canada, federally regulated and private sector businesses subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) are allowed to process or store personal information outside of Canada—provided there are adequate contractual and security safeguards in place and if notice has been given to customers. In Alberta, private sector entities regulated by provincial privacy legislation must go one step further by providing notice (usually via a publicly posted privacy policy) about how to obtain information about the service providers' policies, safeguards, and practices.

The same is not true in the public sector. A major inhibitor to using cloud services are some of Canada's provincial data localization laws, specifically for public sector bodies operating in Nova Scotia and British Columbia, that may limit how personal data can be stored and accessed outside of the country. Both the *Freedom of Information and Protection of Privacy Act* (FOIPPA) in British Columbia and the *Personal Information International Disclosure Protection Act* in Nova Scotia prohibit the access to, disclosure of, and storage of data outside Canada without consent. There may also be other restrictions in Canadian legislation that requires certain records to be kept in Canada (e.g. tax records).

Much of this has to do with the ability of foreign law enforcement agencies to access Canadian citizens' data, without notice or consent, under the *USA Patriot Act*. As a result, Canadian public sector entities have been hesitant to embrace cloud solutions, even where there are no restrictions in other provinces, as a matter of policy. In many cases, additional technologies, such as encryption and tokenization, would need to be considered to enable a public sector entity to use the cloud while still complying with the legislation.

EU laws

Canadian multinationals operating in the EU must pay particular attention to two additional regulatory changes: the invalidation of the US-EU Safe Harbor Agreement [3] and the new General Data Protection Regulation (GDPR) slated to come into force by 2018.

In October 2015, the Court of Justice of the European Union (CJEU) declared the US-EU Safe Harbor Agreement (which enabled data transfers across the Atlantic) invalid on the basis that it could not adequately protect EU citizens' data from being accessed by US law enforcement agencies. This is because EU businesses can only transfer personal information to countries whose laws provide "adequate" protection; the US is not considered to have adequate privacy laws in place. While this ruling does not ban the transfer of data to US-based cloud providers, it does take away the *safe harbour* that companies would have had when transferring personal data from the EU to the US for data storage or processing. This is problematic considering that the top four cloud service providers—Amazon Web Services, Microsoft Azure, Google, and IBM SoftLayer—as well as most major Software as a Service players—such as ServiceNow, Sales Force, and Microsoft Office 365—are all headquartered in the US, with the majority of their data centres also located in the US.

[3]The Safe Harbor Agreement was negotiated between the US Department of Commerce and the European Commission to enable businesses to transfer EU data to the US in compliance with the EU Data Protection Directive (now being replaced by the GDPR). Only organizations that self-certified against Safe Harbor privacy principles were legally permitted to transfer EU data to the US. The CJEU ruling unfolded in a case that was brought by Max Schrems, an Austrian Facebook user who lodged a complaint with the Irish DPA after the Snowden revelations had shown that his data and that of other EU citizens had been accessed by US intelligence services.

In order to provide businesses with a long-term principled-based self-certification scheme to securely transfer personal data of European residents to the US, the European Commission and the US Department of Commerce (DOC) have recently finalized a new agreement called the EU-US Privacy Shield. This agreement includes principles such as security, accountability for onward transfer, notice, choice, data integrity, purpose limitation, access, recourse, enforcement and liability. Under the new framework, companies transferring EU citizen data must commit to stricter data privacy obligations and publish them. These privacy commitments will be overseen by the DOC and enforced by the Federal Trade Commission (FTC). Furthermore, companies processing EU HR data will be bound by the decisions of the European Data Protection Authorities (DPA).

While Canada's PIPEDA legislation is currently considered adequate to protect EU citizens' data, it may be challenged if Bill C-51, Canada's new* Anti-Terrorism Act*, is not amended from its current form, giving Canadian law enforcement agencies broad powers to access foreigners' personal information for national security purposes.

In addition, the new GDPR will place new security and privacy requirements on any organization that uses cloud providers to process and/or store EU citizens' data. Once passed, the GDPR will supersede the European Data Protection Directive, which provided the basis for every data protection law in each member state, and expand the accountabilities for both cloud users and providers, as follows:

- Any company (data controller) that chooses to process data in the cloud will need to ensure that the cloud provider (data processor) offers sufficient guarantees to implement appropriate technical and organizational safeguards that meet the new EU regulation
- The service contract between the data controller and the data processor will need to prohibit further use of subcontractors without consent
- The service contract must mandate the data controller to remove the data from the cloud on termination of the contract, and make available any information to the country's DPA to ensure compliance
- Both data controllers and processors will need to conduct risk assessments to ensure the use of security measures is appropriate to the identified risks
- Data controllers will have a duty to report breaches of security, and both the data controller and processor may be jointly liable for any damages resulting from a breach

It is worth noting that these changes are already having an effect on the market. Both Microsoft and Amazon have announced that they will be opening cloud service centres in Canada to meet the customer demand for in-country data. Microsoft also announced data storage capabilities within Germany using a new encryption control scheme, where a local company holds the security keys for the German servers in its Azure cloud. Only a German court will be able to order these to be surrendered. It is expected that this practice will become standard for sites outside of the United States.

Step 2:

How is your data protected?

Understand how your cloud provider will protect your data

In light of these regulatory trends, Canadian companies using the services of most cloud providers must pay particular attention to the jurisdictions where their data will be stored.

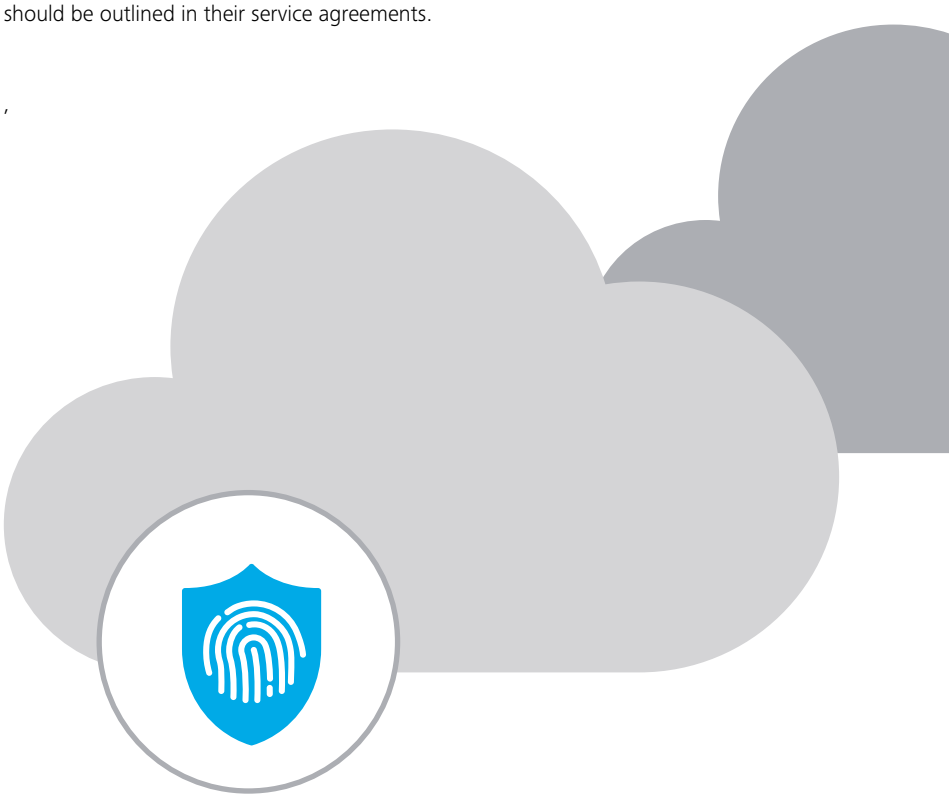
To comply with global privacy regulations, organizations need to ensure that their cloud providers implement technical and administrative controls to protect their data. This is especially critical for organizations that deal with EU data, as EU authorities can assess every single data transfer if a privacy complaint is brought to their attention. To prevent non-compliance, contracts with cloud service providers should define data protection standards and establish Service Level Agreements (SLAs) that outline security and privacy measures. These measures should include adequate technical controls, such as end-to-end encryption or tokenization. Data loss prevention tools can also help enforce policies for data movement.

For these legal agreements to have practical effect, organizations must also actively manage them. In other words, organizations should require regular reports on the adequacy of their providers' privacy and security measures and database activities, as well as disclosure of any incidents or issues that may put data at risk.

Organizations should also have dedicated privacy and security contacts within their cloud service providers to ensure issues, questions, and incidents can be addressed immediately. This is especially important in light of regulations that require companies to report data breaches. This type of mandatory breach reporting is required in 47 US states, as well as throughout Canada and now in the EU in light of the new GDPR. For instance, almost every province has mandatory breach reporting by a custodian for health information, and the *Digital Privacy Act* now requires breach reporting by all private businesses and federally regulated entities (i.e. banks). Moreover, the GDPR will hold both cloud service users and their providers jointly liable for privacy breaches, with breaches having to be reported to supervisory authorities within 72 hours of discovery. This makes it critical for contracts between cloud users and service providers to address breach notification requirements.

Finally, organizations should use reviews, risk assessments or audits to confirm that their cloud provider is meeting the data protection standards set out in their contracts. The GDPR mandates a Privacy by Design[4] approach be taken by embedding privacy into any new technology or service offering and by conducting risk assessments for high-risk data holdings. These can be in the form of third-party audits that the cloud provider makes available to its clients or a Privacy by Design risk assessment that the cloud user conducts itself. In any case, organizations will need to work more closely with their cloud providers to clarify responsibilities for data protection and establish meaningful mechanisms to monitor their providers' activities that should be outlined in their service agreements.

,



[4]Privacy by Design is a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices.

http://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF

Step 3:

How private is your data?

Explore different encryption technologies and tools

When you encrypt data, you render it unreadable without the encryption, and if it's unreadable, cybercriminals won't bother to steal it because it has no value on the black market or to any interested third party[5]

Encryption is a mature set of technologies that can be applied to a cloud solution to increase the security and privacy control over data. Encryption approaches vary, and can be implemented for files, databases, and applications, depending on the need. In some cases, encryption can be done directly via the operating system for all of the system volumes. Data encryption is an explicit feature that your cloud provider may support through a set of services and mechanisms.

Encryption can operate at a number of levels, depending on your requirements, application, and desired approach. Structurally, you will need to consider what mechanisms you want to employ to encrypt your data, and also consider your key management strategy.

Encryption mechanisms. These mechanisms implement the actual encryption algorithm used to hide or obscure data. Most are based on key-based algorithms, using either a shared key or a public/private key pair. Alternatively, tokenization is used—a process that involves substituting specific token fields for anonymous data tokens (which may or may not allow for recovery of the original data). This model is commonly used with applications such as CRM (e.g. Salesforce or Dynamix) as well as other business applications (e.g. credit card data or workforce-management information). Most database software now allows data to be encrypted in the database, and only decrypted when used with an approved application and authorized user credentials. Encryption appliances offer another approach, encrypting data as it leaves a private network and decrypting it when accessed by an approved user.

Your choice of encryption needs to align with the capabilities of the particular application you are using and the cloud service provider being employed. The impact on end-user performance also needs to be considered, as different mechanisms may have significant impact on the user experience. Appliance solutions, for example, require all user data to route through the appliance, which may not scale for very high user volumes. Encryption of the user device may result in slowdowns, since there may be insufficient processing power there.

Key management strategy. This encompasses how you control your encryption keys. Today there are numerous cloud services that offer key management solutions, often as part of a larger overall cloud service suite. The risk of these solutions is that you are still allowing someone else to control the information access. An approach that keeps the keys under your organization's control, either through a key management solution or an encryption appliance, may provide better risk mitigation, especially in jurisdictions that have strict data localization laws.

[5]Forrester (2015, September 10) Wecome to the New Era of Encryption

More work to be done.

As a data custodian or controller, you need to continually review the changing landscape of privacy and security regulations and requirements. As these continue to evolve, so will your strategy. It is important to build regular reviews into your planning cycles for risk and IT. Technology alone won't protect you—your processes and methods must work with the technology and constantly evolve as the requirements and threat landscape change.

Contacts

To learn more about data privacy implications on cloud computing and how we can help your organization, please contact us.

National

Sylvia Kingsmill
National Data Protection and Privacy Leader
skingsmill@deloitte.ca
416-985-1080

East

Amir Belkhelladi
Partner
Cyber Risk Services
abelkhelladi@deloitte.ca
514-393-7035

Robert Masse
Partner
Cyber Risk Services
rmasse@deloitte.ca
514-393-7003

West

Jamie Ross
Partner
Cyber Risk Services
jaross@deloitte.ca
250-978-4412

Tejinder Basi
Partner
Cyber Risk Services
tbasi@deloitte.ca
604-640-3255

For further information on cloud computing solutions, please contact:

David Brassor
Director, Consulting
dbrassor@deloitte.ca
416-874-3150

David Woelfle
Senior Lead, Consulting
dwoelfle@deloitte.ca
416-601-6023

Notes

www.deloitte.ca

Designed and produced by the Deloitte Design Studio, Canada. 16-3723V