

### Azure and Intune can help customers meet their obligations under Canadian privacy laws.

#### Microsoft and Canadian privacy laws

Microsoft Azure and Microsoft Intune are built with established ISO/IEC security standards in mind, and Microsoft maintains technical and organizational measures to protect customer data. These measures comply with the requirements set forth in such established security standards as [ISO/IEC 27001](#) and ISO/IEC 27002, and the code of practice for cloud privacy, [ISO/IEC 27018](#). Microsoft has assessed its practices in risk, security, and incident management; access control; data integrity protection; and other areas relative to the recommendations from the Office of the Privacy Commissioner of Canada, and has determined that in-scope Azure and Intune services can meet those recommendations. This means that Azure and Intune can help customers meet the requirements of Canadian privacy laws.

To support public- and private-sector organizations that are concerned about data sovereignty, Microsoft has established two datacenters in Canada in Toronto and Quebec City. These datacenters add in-country data residency, failover, and disaster recovery for core customer data at rest as defined in the [Microsoft Online Services Terms](#).

To assist Canadian customers who are considering outsourcing business functions to the cloud, Microsoft has published [Navigating your way to the cloud: A compliance checklist for financial institutions in Canada](#). This document provides an overview of the regulatory landscape, including privacy regulations, and a detailed listing of how Microsoft business cloud services can help organizations meet contractual requirements for material outsourcing arrangements.

#### Microsoft in-scope cloud services

- Azure  
[Learn more](#)
- Intune

#### How to implement

- **Privacy at Microsoft**  
Get details on Microsoft privacy principles and standards and on privacy laws specific to Canada.  
[Learn more](#)
- **Compliance checklist: Canada**  
Learn more about Azure and Intune functionalities that can help meet Canadian privacy laws.  
[Learn more](#)
- **Azure data protection**  
Azure provides customers with strong data security, both by default and as customer options.  
[Learn more](#)

#### About Canadian privacy laws

Canadian privacy laws were established to protect the privacy of individuals and give them the right to access information gathered about them. The [Office of the Privacy Commissioner of Canada](#) (OPCC) oversees compliance with these laws.

The [Privacy Act](#) regulates how federal government organizations collect, use, and disclose personally identifiable information including that of federal employees. The [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) governs the same for the business activities of commercial for-profit enterprises and for the employees of federally-regulated businesses like banks, airlines, and telecommunications companies.

PIPEDA is founded on 10 [fair information principles](#) that businesses must follow if they are to comply with it. For example, the basic principle of consent gives rise to the PIPEDA requirement that organizations must obtain an individual's permission to collect or use their personal information. Individuals have the right both to access that personal information and challenge its accuracy (grounded in the principle of "individual access"). The principle of "identifying purposes" leads to the rule that personal information can be used only for the purposes agreed upon.

In general, PIPEDA applies to commercial activities in all provinces and territories, except those operating entirely within provinces with their own privacy laws that have been declared “substantially similar” to the federal law. For example, British Columbia, Alberta, and Quebec have private sector privacy legislation deemed substantively similar to PIPEDA, and as a result the provincial laws are followed there in place of the federal legislation.

## Frequently asked questions

### Can customers using Azure and Intune comply with PIPEDA and other Canadian privacy laws?

Microsoft agrees in its [Online Services Terms](#) that it will comply with laws and regulations that apply to its provision of Microsoft Online Services. However, organizations that leverage Microsoft business cloud services always remain accountable for adherence to Canadian privacy legislation—the laws are clear that organizations are ultimately responsible for ensuring that any sensitive data they gather is fairly handled and adequately protected.

As a result, privacy is a shared responsibility between Microsoft as a cloud service provider and the customer using cloud services. At a high level, this means that customers must ensure that their solutions implemented within Microsoft environments address the 10 principles codified in PIPEDA—for example, getting the consent of individuals to collect their data and safeguarding it with adequate security measures.

### What third-party audits validate the security control environment of Azure and Intune?

Azure and Intune are built on such established security standards as [ISO/IEC 27001](#) and the [SOC framework](#). Their compliance with these standards is confirmed by third-party auditors who provide independent validation that security controls are in place and operating effectively.

Each audit results in the generation of an audit report, which Microsoft makes available either on the [Microsoft Service Trust Portal](#) or at another location. Microsoft will provide audit reports to customers who request them, subject to non-disclosure and distribution limitations of Microsoft and the auditor.

### Will customers know the physical location where their data is stored?

Canadian customers of Microsoft business cloud services will [know where their customer data is stored](#). Furthermore, no matter where customer data is located, Microsoft does not control or limit the locations from which customers or their end users may access their data.

PIPEDA doesn't require Canadian businesses to keep personal information in Canada. However, depending on the province where organizations do business, or their industry, they could be required to keep certain types of data within Canadian borders. To help address these types of requirements, Microsoft has established two datacenters in Canada that support Azure and Intune—in Toronto and Quebec City—and verifies that each datacenter meets stringent security requirements.

## Additional resources

[Summary of privacy laws in Canada](#) (OPCC)

[Privacy at Microsoft](#)

[Microsoft Privacy Statement](#)

[Privacy considerations in the cloud](#)