BRITISH COLUMBIA | Ministry of Citizens' Services

Responsible adoption of cloud in B.C.'s public sector

Ministries and other public bodies in British Columbia are gradually adopting cloud solutions as part of government's digital transformation. Over the next few years, this will only accelerate as cloud solutions become the new norm in the market. Here are the facts:

- The B.C. government uses some of the world's most common cloud products and services, including storage, communication tools and software.
- The use of cloud technology in the B.C. public sector is limited by the *Freedom of Information and Protection of Privacy Act* (FOIPPA). FOIPPA generally requires personal information to be stored and accessed only within Canada, with a few specific exceptions.
- In October 2019, the Ministry of Citizens' Services amended this legislation, adding two new sections that allow personal information to leave Canada for temporary processing. (This type of processing is done automatically by machines in an instant. It is a seamless part of cloud applications and cannot be deactivated.)
- These amendments have implications for the entire B.C. public sector. They remove a barrier to adopting the next generation of cloud-based or cloud-enabled tools – many of which already require or will soon require the temporary processing of data outside Canada.
- These amendments **do not** authorize public bodies to use all cloud services – just those that store data in Canada and otherwise meet the requirements of the new sections and the rest of the Act. These services must also meet the organization's business, security and system requirements.
- Any ministry or organization within the B.C. public sector is able to explore and purchase a cloud solution, **if** that solution meets all business, privacy, security and system requirements. This process involves working with the ministry or organization's privacy, security and procurement experts to apply the necessary due diligence and select a vendor. This typically includes:
    - A Privacy Impact Assessment (used to evaluate and manage privacy impacts and to ensure compliance with privacy protection rules and responsibilities)
    - A Security Threat and Risk Assessment (used to assess digital risks), and
    - A procurement vehicle (e.g., Request for Proposals)
- Ministries and organizations can see the latest tools available and already assessed for use on the government's Secure Cloud webpage, which will be updated as new applications become available.
- To work with a ministry or public sector organization in B.C., cloud service providers must agree to detailed security requirements in their contracts. At a high level, these requirements include:
    - Complying with an established cloud security framework;
    - Undergoing annual third-party audits to demonstrate compliance with this framework, while giving government the right to audit components; and
    - Enabling security investigations, online access to evidence, and legal discovery.

Learn More:

- For more information, visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/secure-cloud
- For advice on interpreting the amendments to the *Freedom of Information and Protection of Privacy Act* amendments, visit: https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/disclosure-inside-outside-canada#Interpretation
- For information on contract requirements, read the Office of the Chief Information Officer's Security Schedule for Cloud Services online and download the Cloud Privacy Protection Schedule.

March 2020