a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Office of the University Counsel
6328 Memorial Road
Vancouver, BC Canada V6T 1Z2

Phone 604 822 2451
Fax 604 822 8731
access.and.privacy@ubc.ca

Privacy Fact Sheet

Disclosing Personal Information Outside Canada

Introduction

1. Public bodies in British Columbia, including UBC, are required to exercise particular vigilance before disclosing personal information to be stored outside Canada. The Office of the University Counsel has developed this Privacy Fact Sheet to explain the procedure that faculty and staff members must follow before storing personal information outside the country.

2. This Privacy Fact Sheet is not a substitute for legal advice. If you have questions about a specific situation, contact the Office of the University Counsel.

Implications for Cloud Services

3. Many computing services are offered through the Internet, and may be hosted in the United States or other foreign jurisdictions. Using these services to collect, store, transmit or access personal information raises special concerns so it is preferable, where reasonably possible, to use a Canadian-based alternative.

4. Here are some examples of commonly used cloud services, with Canadian-based alternatives:

Cloud Services	Canadian-based Alternatives
Dropbox	OneDrive
Gmail, Hotmail	FASmail
Survey Monkey	UBC Survey Tool
Google Docs	Microsoft Word and Excel

5. If you are able to a Canadian-based tool like the above examples, you should do so. If there are no reasonable alternatives in Canada and you would like to use a foreign-based tool, you must request a privacy impact assessment (PIA) to determine whether it is safe to do so. You must not proceed until you have received the results of the PIA.

Privacy Impact Assessments

6. Under the *Freedom of Information and Protection of Privacy Act* (FIPPA), all initiatives that involve the collection, use or disclosure of personal information must undergo a PIA. The purpose of a PIA is to identify and assess privacy risks and identify measures that are proportionate to the level of the risk.

7. If the initiative involves the disclosure of sensitive personal information for storage outside of Canada, an additional assessment must be conducted through the PIA process to identify the privacy risk(s) associated with the disclosure. “Sensitive” personal information includes information such as personal health information, date of birth, or government identity card information. The purpose of this additional assessment is to ensure that the information will remain secure if stored outside Canada.

8. For each privacy risk, the PIA must identify a response that is proportionate to the level of risk posed. These responses may include technical, security, administrative or contractual measures (e.g. ways to manage and review access to personal information). If it is not possible to identify adequate responses to protect the information, the initiative will not be permitted to proceed.

9. It is important to note that UBC is legally required to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal.[1] This would normally prevent UBC from processing or storing personal information in a jurisdiction that does not respect the rule of law, or that has inadequate or non-existent privacy laws.

10. PIAs are conducted by the Privacy Matters team. To request a PIA, refer to https://privacymatters.ubc.ca/privacy-impact-assessment.

[1] FIPPA section 30