OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Reasonable security measures for personal information disclosures outside Canada

March 2022

Introduction

In November 2021, the data residency provisions of the *Freedom of Information and Protection of Privacy Act* (FIPPA) were amended to remove the prohibition (with certain exceptions) on disclosure of personal information outside of Canada. The new legislative framework permits the disclosure of personal information outside of Canada in accordance with B.C. Reg. 294/2021.[1] And critically, public bodies' obligations under s. 30 of FIPPA to implement reasonable security measures continue to apply to any disclosure of personal information outside Canada. Therefore, a careful assessment under s. 30 is necessary before any disclosure of personal information outside of Canada.

This guidance is intended to help public bodies interpret their s. 30 obligations when deciding whether to disclose or store personal information outside Canada. This guidance only relates to s. 30. It does not deal with any obligations for disclosure of personal information outside of Canada under s. 33.1 or B.C. Reg. 294/2021.

The need for authority to disclose personal information outside Canada

A key point: public bodies can only disclose personal information if FIPPA authorizes it. It is particularly important that public bodies have clear authority for disclosures outside of Canada. The disclosure authority must be in FIPPA, not foreign law.

Also, once personal information leaves the country, Canadian laws do not apply and contractual or technical protections may not be enough to protect the information adequately. Because of that reality, carefully considering—in a privacy impact assessment—whether you should disclose personal information outside the country is an important aspect of the s. 30 requirement to protect personal information.

Reasonable security measures to protect personal information

Section 30 requires public bodies to implement "reasonable security measures" to protect personal information in their custody or control[2] against risks such as unauthorized collection, use, disclosure or disposal. This duty applies to disclosure or storage of personal information outside Canada. Public bodies should employ administrative, technical or contractual controls and should be prepared to demonstrate reasonable security controls in line with industry standards such as ISO 27002, ISO 27017 or the NIST Cybersecurity Framework. For more information, see the OIPC's security self-assessment tool.[3]

---

[1] The Personal Information Disclosure for Storage Outside of Canada Regulation

[2] This includes personal information held by a public body service provider.

[3] See British Columbia, Office of the Information and Privacy Commissioner *Securing personal information: A self-assessment tool for public bodies and organizations*, (B.C, OIPC, 2020).

The meaning of "reasonable" for disclosures outside Canada

The standard of reasonableness in the context of s. 30 has been interpreted by the Office of the Information and Privacy Commissioner (OIPC) as follows:

> [49] By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.[4]

Disclosure of personal information outside of Canada requires a very high level of rigour. This is due in part to the fact that the consequences of unauthorized disclosure outside of Canada may be more serious than within Canada.

Assessment factors for determining whether to disclose outside Canada

At a minimum, any security risk assessment involving disclosure outside Canada must include an assessment of the legal framework in the jurisdiction where personal information is being disclosed.

It is unlikely that a public body would be able to meet its obligations under s. 30 when information under its control is processed or stored in a jurisdiction that does not respect the rule of law, has no privacy laws, or those laws are inadequate. Hallmarks of jurisdictions respecting the rule of law include an independent judiciary, constitutional individual freedoms, due process, and responsible government. For example, a data protection statute under an authoritarian governing structure that has the power to compel information without a warrant would not be considered adequate.

Other factors that should be assessed, depending on the circumstances, include:

- the sensitivity of the personal information in question (e.g., personal health information is much more sensitive than contact information);
- the volume of the personal information in question;
- the foreseeability of an unauthorized collection, use, disclosure, or storage of personal information;
- the impact to individuals of an unauthorized collection, use, disclosure, or storage of their personal information;
- whether the personal information is stored by a service provider; and

[4] Investigation Report F06-01, <https://www.oipc.bc.ca/investigation-reports/1232>, reiterated in Investigation Report F11-01 Investigation into a Privacy Breach of Customers' Personal Information by the British Columbia Lottery Corporation (Re), 2011 BCIPC 6 (CanLII), <https://canlii.ca/t/2fxmt>.

- whether a reasonable alternative is available within Canada.

Even if the relevant factors suggest that the disclosure outside Canada is reasonable, s. 30 also requires public bodies to implement reasonable administrative and technical measures to protect the information in accordance with the risks involved.[5]

In summary, the new discretion to disclose personal information outside Canada demands a very high level of rigour and should only be undertaken after a careful assessment. Disclosure outside Canada will always involve risks that no administrative, technical and contractual controls can eliminate. Therefore, public bodies should only disclose personal information outside of Canada if, objectively, the risks involved are reasonable and, additionally, there are reasonable measures in place that adequately mitigate those risks.

For more information, or to consult with the OIPC, please contact us at (250) 387-5629 or info@oipc.bc.ca.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA.

[5] Examples include encryption in transit and at rest abroad, contractual restrictions on further use or disclosure by a service provider, contractual duties for service providers to report breaches, cure them, and much more.