Goodmans LLP

Privacy Commissioner Reverses its Position on Cross-Border Transfers of Personal Information

April-15-2019

Lawyer Niki Kermani, Monique McAlister, Peter Ruby
Area Litigation, Privacy Law

Summary

Download PDF

Last week the Office of the Privacy Commissioner of Canada (the "**OPC**") launched a "Consultation on transborder dataflows" (the "**Consultation**"), in which it proposes to totally reverse its policy position on cross-border data transfers by organizations subject to the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"). In the absence of an applicable exception under PIPEDA, the OPC's revised view is that the transfer of personal information for processing, including a cross-border data transfer or the transfer of personal information to an affiliated corporation, is a "disclosure" of personal information that requires consent.

The OPC's new proposal is a departure from its previous position. Up until the release of the Consultation and the OPC's accompanying report of findings in its investigation into the 2017 Equifax breach (the "**Equifax Report**"), the OPC's policy position has been that a transfer of personal information for the purpose of processing is a "use" rather than a "disclosure" of personal information. The implication of such a transfer being a "use" is that transferring organizations are required to provide notice to affected individuals, while the main implication of that transfer being a "disclosure" is that the organization requires consent of the individual for the transfer.

The reason given by the OPC for this policy change is that under PIPEPA, any collection, use or disclosure of personal information requires consent, unless an exception to the consent requirement applies. Since "nothing in PIPEDA exempts data transfers, inside or outside Canada, from consent requirements", the OPC's updated view is that, "as a matter of law, consent is required".

The OPC intends to provide guidance on disclosures for processing and related consent and accountability requirements. It is seeking input on its updated policy position, as well as on specific areas for which related guidance would be most needed. Comments are due by **June 4, 2019**.

The cross-border disclosure of personal information, including for processing, requires consent

The Consultation also highlights the importance of obtaining meaningful consent. For consent to be valid, organizations must provide individuals with clear information regarding any disclosure to a third party, including instances when they are located in another country, and the associated risks.

In determining whether express or implied consent is appropriate, companies should consider the sensitivity of the information and the individuals' reasonable expectations in the circumstances; underlying both should be a consideration of the risk of harm to the individual. The OPC notes that "where there is a meaningful risk that a residual risk of harm will materialize and will be significant, consent should be express, not implied". In the OPC's view, "individuals would reasonably expect to be notified if their information was to be disclosed outside of Canada and be subject to the legal regime of another country."

Individuals must be informed of any options available if they do not consent to cross-border disclosures of their personal information

Individuals must be provided with clear and adequate information about the nature, purpose and consequence of any cross-border disclosure of personal information, so they can make an informed decision about whether to consent to the disclosure. Where the disclosure is not necessary to provide a product or service, individuals must be provided with a clear and easily accessible choice regarding the disclosure. However, where the transfer for processing is "integral to the delivery of a service", organizations are not obligated to provide an alternative.

The OPC did not specify a test for what is "integral to the delivery of a service".

When disclosing personal information to a third party for processing, a company does not relinquish control of the information

An organization that transfers personal information for processing will generally remain accountable for the personal information as the "controller". The Consultation notes that determining which organization has personal information "under its control" can be complex and must be assessed on a case-by-case basis. The OPC will look at factors such as contractual arrangements, commercial realities, evolving business models and shifting roles when determining which organization "controls" the personal information. As is currently the case, the controller will still be required to use contractual or other means to provide a comparable level of protection while the information is being processed.

The OPC's finding about the Equifax breach illustrates this accountability.

The OPC found that Equifax Canada remained accountable for the handling of Canadian personal information by Equifax Inc. The OPC determined that for the purposes of personal information handling under PIPEDA, Equifax Inc. is considered a "third party" to Equifax Canada because: (a) they are separately incorporated in different jurisdictions; (b) although both the Privacy Policy and Terms of Use available to Canadians at the time of the breach make reference to the possibility of Equifax Canada partnering with affiliates in the delivery of products, they are separate entities; and (c) Equifax Canada has consistently represented that its Chief Privacy Officer is the designated individual accountable for the handling of personal information by Equifax Canada.

The OPC also found that "to determine the appropriate levels of controls, consideration must be given to both the scope and sensitivity of personal information being handled". In some cases "where the third party is closely affiliated and the personal information being handled is of limited scope and sensitivity, it may be possible to rely on light controls and pre-existing, adequate, policies and practices of the third party" to fulfil the accountability obligations of the controller. However, where a substantial volume of sensitive personal information belonging to a large number of individuals is being handled over a prolonged period, the level of

controls should be “commensurately high”, including at a minimum: (a) a formal written arrangement, updated periodically and in the case of material changes; and (b) a structured program for monitoring compliance against the obligations laid out in the arrangement that is suitable to the scope and sensitivity of the personal information being handled.

Ultimately, the OPC concluded both Equifax Inc. and Equifax Canada contravened PIPEDA due to: (a) inadequate data protection safeguards by both companies; (b) inadequate accountability by Equifax Canada with respect to Canadian data processed by Equifax Inc.; and (c) the failure of Equifax Canada to obtain valid consent from individuals whose personal information was transferred to Equifax Inc. for processing and was eventually compromised.

Implications for Businesses

The OPC’s shift in its position suggests a progression in aligning PIPEDA with the European Union’s General Data Protection Regulation and Canada’s international trade obligations. In setting out its revised policy position on cross-border data transfers, the OPC notes “organizations are free to design their operations to include flows of personal information across borders, but they must respect individuals’ right to make that choice for themselves as part of the consent process.” While “individuals cannot dictate to an organization that it must design its operations in such a way that personal information must stay in Canada (data localisation)”, at the same time “organizations cannot dictate to individuals that their personal information will cross borders unless, with meaningful information, they consent to this.”

As data transfers for processing are now considered third-party disclosures, regardless of whether the transfer is to a third party or an affiliate company, organizations should re-examine their consent processes and privacy policies. To obtain valid consent, organizations should provide clear and adequate information about the nature, purpose and consequence of any transfer of personal information to a third party, including instances when they are located in another country, and the associated risks. Where the information will be disclosed outside of Canada, individuals should be informed their personal information may be subject to the legal regime of another country. Where the disclosure is not necessary to provide a product or service, individuals must be provided with a clear and easily accessible choice regarding the disclosure.

Companies should also ensure they enter into data processing agreements that impose sufficiently robust obligations on recipient organizations, including for intercompany transfers of personal information between affiliated entities. Where a substantial volume of sensitive personal information belonging to a large number of individuals is being handled over a prolonged period, the parties should have in place: (a) a formal written arrangement, updated periodically and in the case of material changes; and (b) a structured program for monitoring compliance against the obligations laid out in the arrangement that is suitable to the scope and sensitivity of the personal information being handled.

For further information on the OPC’s revised policy position or opportunities to comment on the Consultation, please contact any member of our Privacy Law Group.

Download PDF