Cassels

Privacy Commissioner Reverses Course - Consent Required for Personal Information Processing

Bernice Karn

April 16, 2019

Last week, the Office of the Privacy Commissioner of Canada (OPC) issued its investigation report into the 2017 Equifax security breach and concurrently announced that it would be conducting a public consultation on transborder data flows. In making the announcement, the OPC acknowledged that its findings on the issue of consent in cases of transfers for processing represent a marked departure from its previous guidance in this area.

Transfers for Processing vs. Disclosures

In this digital age, processing and storage of data are functions that are frequently performed by third party service providers on behalf of organizations. In some cases, the service providers are unrelated to the organization, while in other situations, affiliated entities perform these services. Additionally, these types of services may be outsourced to organizations in low cost jurisdictions or, in the case of global entities looking to achieve economies of scale, consolidated by an organization at the head office level, often in the United States.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not explicitly regulate outsourcing arrangements per se, nor does it contain any prohibition on transferring personal information outside of Canada. Until now, based on the application of the PIPEDA "Accountability" principle in findings and guidance issued by the OPC, organizations have justified providing personal information to third parties for processing without consent on the basis that the processing is not a “disclosure” within the ambit of PIPEDA, but, rather, is a continuation of the “use” by the organization, albeit a use that is carried out by another entity on behalf of the organization.

The “Accountability” principle of PIPEDA, found in Schedule 1, clause 4.1.3, of PIPEDA states:

> *An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.*

In 2009, the OPC issued guidance entitled “Guidance for Processing Personal Data Across Borders”[1] in which the OPC defined a transfer as “*a use by the organization. It is not to be confused with a disclosure*.” The OPC went further and clarified that “*PIPEDA does not distinguish between domestic and international transfers of data*,” and, most importantly, the OPC made explicit that, as long as the personal information is being used for the purpose for which it was originally collected, “*additional consent for the transfer is not required*.” The 2009 guidance suggested that, as long as appropriate safeguards and oversight were in place regarding the processing of personal information by third parties, consent of the applicable data subjects to that transfer was not required. The OPC has now walked back that advice.

Equifax Investigation

In 2017, Equifax Inc. announced a data breach that affected the personal information of more than 143 million individuals worldwide. Of that number, there were approximately 19,000 individuals with Canadian credit files. According to the OPC’s report, almost all of those affected individuals had their social insurance numbers and accompanying identifiers compromised.

The OPC’s investigation into the 2017 Equifax data breach dealt with a number of different issues regarding the handling of personal information held by Equifax Canada Co. (Equifax Canada) and its US parent company, Equifax Inc., namely:

1. Safeguards for Canadian personal information held by Equifax Inc.

2. Retention of personal information by Equifax Inc.

3. Accountability of Equifax Canada for Canadian personal information handling by Equifax Inc.

4. Consent obtained from Canadians for disclosure of information to Equifax Inc.

5. Safeguards of personal information by Equifax Canada

6. Adequacy of post-breach safeguards to protect against unauthorized use.

The third and fourth issues are of particular concern for any organization that uses third parties to process personal information and has relied on the existing OPC guidance that consent is not required for this processing.

In its report on the Equifax Inc./Equifax Canada investigation, among its many findings, the OPC said:

1. Equifax Inc. was considered as a “third party” to Equifax Canada because the entities were separately

incorporated in different jurisdictions, the terms of use on the Equifax Canada website made it clear that Equifax Inc. and Equifax Canada were separate entities, and Equifax Canada had consistently represented that its Chief Privacy Officer was the person designated as accountable for the handling of personal information by Equifax Canada.

2. The "transfers for processing" of personal information from Equifax Canada to Equifax Inc. "constitute disclosures of personal information" within the meaning of Section 7(3) and clause 4.3 to Schedule 1 of PIPEDA.

In its report, the OPC acknowledged, both in the body of the report and its endnotes, that its previous guidance characterized transfers for processing as a "use" of personal information rather than a disclosure and that such transfers "in of themselves" did not require consent. The endnotes also state that, "In the interest of clarity on a going forward basis, we intend to provide further guidance in relation to consent for disclosures which also constitute transfers for processing." To this end, the OPC has issued the "Consultation on transborder dataflows"[2], under which it will be accepting submissions on the issue until June 4, 2019.

Consultation on Transborder Dataflows

In its call for submissions, the OPC has signaled that certain key points inform its change in position on third party processing. The OPC states that "*A company that is disclosing personal information across a border, including for processing, must obtain consent*." This right of individuals to consent now applies to transfers for processing in addition to transactions more traditionally thought of as actual disclosures. Although the consultation is billed as applicable to transborder dataflows, and that certainly is an area of major concern, the OPC makes clear that "*nothing in PIPEDA exempts data transfers, **inside or outside Canada**, from consent requirements*" (emphasis ours).

The consent must be meaningful in that its form depends on the sensitivity of the information and the individual's reasonable expectations in the circumstances. Consistent with its latest thinking on consent[3], the OPC is of the view that express consent is required where there is a meaningful risk that a residual risk of harm might result from the disclosure and that the harm will be significant. Where processing by a third party is "integral to the delivery of a service", organizations are not obligated to provide a Canadian processing alternative, but by the same token, individuals should be given "*clear and adequate information about the nature, purpose and consequence of any disclosure of their personal information across borders*" and, as a result, individuals will be able to make informed decisions about whether or not to do business with the organization.

In terms of cross border considerations, the OPC has reiterated its long held view that individuals should be notified if their personal information will be disclosed outside of Canada and that it will be subject to the laws of the recipient jurisdiction.

Lastly, the OPC has re-emphasized the accountability principle, and the concept that an organization disclosing personal information for processing remains accountable for it. Interestingly, the OPC seems to have borrowed a page from the EU's *General Data Protection Directive*, which imposes obligations directly on data processors (in addition to controllers), by stating that: "*An organization that processes personal information on behalf of another organization may still have obligations under the Act in respect of the personal information in its possession or custody, as an organization that collects, uses or discloses personal information in the course of commercial activities*."

Conclusion

The OPC's new interpretation of the necessity to obtain consent in third party processing situations upends ten years of reliance on previously settled guidance applicable to outsourcing arrangements, whether those arrangements are between related or arm's length entities and whether those arrangements involve the cross border transfer of personal information or are domestic outsourcings. At this point, it is unclear whether the OPC will ultimately approve of any form of "grandfathering" for existing data processing deals or if some type of notice and opt out consent regime will be acceptable for existing and future data processing deals.

Given the significant investments that have been made and continue to be made by organizations for the processing of personal information by third parties, we strongly urge all affected organizations to respond to the call for submissions. As noted above, the deadline is **June 4, 2019**, and submissions may be sent to the OPC at OPC-CPVPconsult2@priv.gc.ca.

We will continue to monitor this matter and provide updates.

For further information regarding this matter, please contact Bernice Karn or any other member of the Information Technology & Data Privacy Group.

---

[1] Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders*, (Ottawa: OPC, January 2009), online: <https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/>.

[2] Office of the Privacy Commissioner of Canada, *Consultation on Transborder Dataflows*, (Ottawa: OPC, 9 April 2019), online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/>.

[3] Office of the Privacy Commissioner of Canada, *Guidelines for Obtaining Meaningful Consent*, (Ottawa: OPC, 24 May 2018), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/