Cassels

Privacy Commissioner Backs Down on Transfers for Processing

Bernice Karn

September 24, 2019

Earlier this year, the Office of the Privacy Commissioner of Canada (OPC) surprised many in the business community by floating the idea of requiring data subjects' consent when transferring personal information to service providers for processing, cross-border or otherwise. This new twist on the *Personal Information Protection and Electronic Documents Act* (PIPEDA) would have reversed ten years of settled guidance from the OPC on the issue. Accordingly, the OPC launched an initial public consultation on the topic and then "reframed" the discussion after the Minister of Innovation, Science and Economic Development issued the federal government's *Strengthening Privacy for the Digital Age* whitepaper in which the Minister seemed to take the view that transfers for processing did not require consent as long as accountability for the use of the information was maintained. (See our summary of these events here.)

Thankfully the OPC announced on September 23, 2019, that, following this consultation, it has concluded that its *Guidelines for Processing Personal Data Across Borders* (Guidelines) from January of 2009 will remained unchanged. These Guidelines instead consider processing by a service provider to be a "use" of the information on behalf of the organization that has transferred it; they focus on transparency and accountability to protect information from unauthorized uses and disclosures while in the hands of a third-party processor. The Guidelines also emphasize that, for cross-border transfers, organizations need to "make it plain" in "clear and understandable language" at the time of collection that personal information may be processed in foreign countries and that it "may be accessible to law enforcement and national security authorities of that jurisdiction."

The handling of personal information by service providers is clearly on the OPC's radar. Prior to the launch of the consultation, the OPC issued its report into the Equifax data breach (PIPEDA Report of Findings #2019-001, April 9, 2019). In this report, included among the many recommendations were the OPC's views on the minimum measures that organizations had to take to comply with clause 4.1.2 of the Accountability Principle in PIPEDA. The OPC stated, in paragraph 74 of the Equifax report:

a. In a case 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.

In such a situation, in our view, PIPEDA Principle 4.1.3 requires, at a minimum:

i. A formal written arrangement, updated periodically and in the case of material changes, which should generally include details about the following:

ii. what personal information is being handled by the third party, including both information shared by the organization and any information collected directly by the third party on behalf of the organization;

iii. what specific rules, regulations and standards need to be complied with in the handling of the information, including PIPEDA;

iv. the roles and responsibilities of key stakeholders within both organizations for the handling of the personal information, including responsibilities for specific functions, decision-making, safeguards and breach response;

v. information security obligations;

vi. acceptable uses of the information;

vii. retention and destruction obligations; and

viii. reporting and oversight arrangements to ensure compliance with the above, including reporting obligations in the case of a breach that could compromise the personal information.

b. A structured program for monitoring compliance against the obligations laid out in the arrangement. The program should be suitable to the scope and sensitivity of the personal information being handled. It should include:

i. mechanisms for periodic reporting by the third party on the handling of the personal information; and

ii. where scope and sensitivity of the personal information handled is significant, mechanisms to ensure periodic external assessment (by the organization or an appropriate third party) of compliance with the full range of obligations described in the written arrangement.

While the OPC seems to have backed off for now from the consent requirement for processing of personal information by service providers, it has served notice that it expects PIPEDA to be “reformed” at some point

in the future and that it is taking a pragmatic “status quo” approach for the time being until the law is finally amended. Although this issue is in abeyance for now, expect it to arise again in the future. Organizations should be reviewing the existing guidance now to plan for potential system/business process changes down the road.

We will continue to monitor the situation as it unfolds.

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