Cassels

Privacy Commissioner Confirms Original Outsourcing Guidance

Bernice Karn

August 10, 2020

On August 4, 2020, the Office of the Privacy Commissioner of Canada (OPC) released a set of findings[1] concerning a decision by TD Canada Trust (TD) to outsource its processing of fraud claims to a third-party service provider located in India. The findings are notable because they represent a departure from recent commentary by the OPC on a possible requirement to obtain consent for outsourcing of personal information processing and a return to the OPC's long-standing position on this issue.

Background

As we reported in a previous articles (on April 16, 2019; June 12, 2019; and September 24, 2019), the OPC surprised many in the business community by announcing a consultation on transborder data flows that proposed a potential requirement to obtain consent of data subjects to the outsourcing their personal information to third party service providers. Prior to this consultation, the OPC's guidance concerning the "Accountability" principle in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) had been that transfers of personal information to service providers were permitted without obtaining consent, as long as the organization engaging the service provider remained accountable for the use of the information and ensured that the information remained subject to a comparable level of protection while in the hands of the service provider. The April 2019 consultation paper proposals would have reversed this accepted guidance.

The OPC subsequently "reframed" this 2019 consultation before ultimately announcing on September 23, 2019, that, following the consultation, it concluded that its previous *Guidelines for Processing Personal Data Across Borders* (Guidelines) from January of 2009 would remained unchanged. Those Guidelines considered processing by a service provider to be a "use" of the information on behalf of the organization that has transferred it; they focused on transparency and accountability to protect information from unauthorized uses and disclosures while in the hands of a third-party processor. The OPC has now revisited the issue in a new set of findings concerning a complaint lodged by a former employee against TD.

The Complaint

A former employee of TD's Fraud Claims Department complained to the OPC that TD had outsourced

certain functions of its fraud claims processing services to a third-party service provider in India without customer consent and without offering the ability for customers to opt out of the transfer of their personal information to the service provider. In addition, the complainant alleged that TD was not sufficiently open about this activity. The OPC also investigated whether TD had met the Accountability principle under PIPEDA to ensure that the service provider provided a comparable level of protection for the personal information in issue.

The OPC found the complaint to be ***not well-founded*** for the following three reasons:

- TD had already collected its customers' consent to use their personal information to manage fraud claims; the use by the service provider on behalf of TD for this purpose was essentially a use of the information by TD and did not require an additional consent. In addition, TD was not obligated to provide an opt-out of the transfer. The OPC pointed to the Guidelines and noted that "once an informed individual has chosen to do business with a particular company, they do not have an additional right to refuse to have their information transferred."
- TD met the "Openness" principle in PIPEDA by providing its customers with information pertaining to its transfers of personal information, including to service providers in other jurisdictions. This information was provided in a variety of ways, such as through its account opening agreements, orally when an individual applied by telephone, through materials available at its bank branches and on its website. The OPC also stressed that this information was made readily and prominently available in clear and understandable language and that it specifically disclosed that the information may be transferred to third party processors in foreign jurisdictions.
- TD also met the Accountability principle in PIPEDA by ensuring a comparable level of protection for the information via a "robust contract" as well as through other methods, such as audits.

Key Takeaways

While these findings represent a welcome return to the OPC's Guidance document about consent in the context of outsourcing agreements, the case is important for any organization seeking to outsource the processing or storage of personal information because it describes the practical measures that TD put into place in order to ensure that the service provider in fact adhered to the contractual restrictions. These measures are particularly important when engaging a service provider to handle sensitive personal information.

The OPC has made clear that simply contractually requiring the service provider to comply with Canadian privacy laws is not sufficient to meet an organization's "Accountability" obligations under PIPEDA; organizations must be more prescriptive in their agreements concerning privacy obligations and should actively monitor compliance. Therefore, clients need to consider building the following concepts into their outsourcing agreements, depending on the sensitivity of the information in issue and the type of services

provided:

- Explicitly prohibit the service provider from using or disclosing the personal information it accesses for any purposes other than those set out under the contract;
- Where feasible, provide the service provider with limited, “view only” remote access to the personal information in an environment controlled by the organization; do not permit the service provider to retain any copies of the personal information it is processing;
- Implement the following measures to safeguard the personal information:
    - Conduct a risk assessment prior to entering into the contract, which would include pre-contractual due diligence on the service provider;
    - Implement any applicable regulatory requirements, guidance, and industry best practices; conduct a privacy impact assessment; obtain legal advice, including, where applicable, on the impact of foreign laws on the processing of personal information in a foreign country, and incorporate the results of the risk assessment activities into the eventual outsourcing agreement;
    - Require that the service provider conduct employee background assessment and monitoring, both prior to entering into the contract and annually thereafter, and revoke access to any employees who fail the background investigations;
    - Require that the service provider maintain policies, training and regular testing on the handling of the outsourcing organization’s information in accordance with the outsourcer’s policies and procedures, and that the service provider require compliance with those policies and procedures;
    - Employ physical work environment controls designed to prevent unauthorized handling and storage of the organization’s information, such as maintaining an access-controlled, windowless, monitored, paperless “clean room” working environment, in which any employee electronic devices or writing instruments are prohibited;
    - Mandate access and other cybersecurity controls such as:
        - supplying hardware and software to the service provider for use only in the “clean room”;
        - providing access to the organization’s environment and information through a remote web-based gateway platform;
        - limiting databases to information required for specific tasks and incorporating a role-based access permissions model;
        - implementing two-factor authentication;
        - limiting access to “read only” as necessary to perform required tasks;
        - partially masking certain sensitive personal information such as a SIN or date of birth;
        - limiting activities that service provider employees can conduct in the organization’s technology environment, such as restricting access to unauthorized URLs, limiting external emails and disabling any print, cut, copy, screenshot, or similar capabilities;
        - requiring the service provider to monitor its employees’ activities electronically,

including through the use of computer access monitoring and audit logs;
- requiring the service provider to maintain a formal program to ensure malicious software protection is in place; and
- requiring the service provider to perform industry standard security and intrusion testing, including attack and penetration testing, at least annually.

- Proactive monitoring and enforcement of contractual obligations, including:
  - contractually mandating regular audits by an independent auditor of the service provider's practices, which should include security and access monitoring;
  - requiring any issues identified during the course of any audit to be remediated and have the remediation monitored and approved by an independent auditor; and
  - requiring the service provider to attest annually that it meets all contractual obligations.

Of course, these types of measures are quite expensive to implement and in many types of outsourcing arrangements the customer organization will not have enough negotiation leverage to demand these types of extensive privacy protections. Additionally, in cloud services outsourcing deals, the point of engaging the service provider is to take advantage of the service provider's lower cost technology environment based on economies of scale. In that case, it is unrealistic to think that the customer organization would be able to introduce many of these types of measures, since the customer is but one of many sharing a technology platform operated by the service provider. However, it is always prudent to conduct extensive due diligence on service providers who are handling personal information, make an informed decision on vendor selection, require compliance with basic privacy protections and obtain some form of audit comfort, whether through on-site investigations or industry standard reporting.

---

[1] Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2020-001", (August 4, 2020) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-001/>.
