INTRODUCTION AND OVERVIEW:

The *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 (“*PIPEDA*”), and private sector privacy legislation in Alberta, British Columbia, and Quebec, (collectively, “Canadian Privacy Legislation”) govern the collection, use and disclosure of employee data by private sector organizations. The application of Canadian Privacy Legislation in the employment context is not straightforward, and can often lead to confusion for both employers and employees about how and whether their interests will be protected. In particular, Canadian Privacy Legislation must be considered when the storage and maintenance of employee data is at issue. Increasingly, large businesses are storing such records in one location in order to avoid duplication of efforts and to enhance data protection measures. While this practice may make good business sense, the transfer of Canadian employee data, especially to third parties outside Canada’s borders, triggers significant privacy concerns.

This article will highlight requirements articulated by Canadian Privacy Legislation regarding the disclosure of employee data across borders for processing and storage. These requirements usually differ depending on the originating jurisdiction of the employee data. While it is beyond the scope of this article to provide a complete survey of the law in this area, this article will focus on measures all organizations can implement when proposing to transfer information to third parties outside Canada for the purposes of administering the employer/employee relationship.

The three predominant issues that should be considered when advising clients on the transfer of employee data outside Canada are: (i) Which statute, if any, is applicable to the transfer of employee data?; (ii) Is employee consent required?; and (iii) What type of contractual considerations should be included in a processing contract with third party data recipients?

(a) Applicable Law

In order to determine the legality of the disclosure of employee data to a third party, counsel first needs to determine which piece of Canadian Privacy Legislation governs the employee data. In order to do so, the following questions should be considered:

1) Whether the employee data at issue constitutes personal information and/or personal employee information;
2) Whether or not the disclosure of employee data occurs in the course of commercial activity; and
3) Whether the organization is subject to federal or provincial authority.

It is also practical for counsel to consider whether the relevant privacy commissioner’s office has jurisdiction to address the disclosure.

(b) Form of Consent

When considering what form of employee consent is required it is important to note that PIPEDA is more stringent in this regard than Alberta’s PIPA or B.C.’s PIPA. Pursuant to PIPEDA, the collection, use and disclosure of the personal information of employees in federally-regulated organizations requires the consent of their employees with respect to the collection, use and disclosure of personal information. The privacy legislation in Alberta and British Columbia, however, has separate rules for the collection, use and disclosure of information in the employment context whereby consent is not required. Similarly, the Quebec Act includes a provision that permits personal information, which encompasses employee personal information, to be disclosed...
outside Quebec if the organization that has disclosed the information takes reasonable steps to ensure that the personal information is not used for purposes irrelevant to those for which it was initially collected.

Canadian Privacy Legislation is primarily consent-based. Accordingly, the most effective way to prevent a complaint when the collection, use and disclosure of personal information is at issue is to seek the express consent of the individual whose personal information is subject to disclosure. Given that this approach is not likely to be practical in certain instances, organizations should ensure that they provide clear notification to their employees when planning to transfer and disclose employee data to third parties outside Canada for processing and storage.

Organizations should be advised to revise and re-distribute their employee privacy policies to account for changes to the storage of employee data, and to ensure notice and transparency in this regard. Employees should be notified in a manner which indicates the type of personal information that is at issue, or the organization should at least provide contact information where this information can be obtained. Further, employees should be informed of the purposes for which their employer wishes to disclose their personal information to a third party. This notification should include a method for the employee to contact his or her employer, including a telephone number or e-mail address of the designated contact person or privacy officer, to inquire about the disclosure of their personal information. It is also recommended that employees be informed about the possible risk to their personal information when it is transferred outside Canada.

(c) Processing Contracts with Third Parties

Under PIPEDA, an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. Accordingly, it is the responsibility of the originating organization to use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. The Office of the Privacy Commissioner has endorsed contract terms which include:

- Guarantees of confidentiality and security of personal information;
- Oversight, monitoring and auditing of the services being provided;
- Details pertaining to the third-party service provider’s security policy.

CONCLUSION:

The application of Canadian Privacy Legislation in the employment context is not a straightforward task, because (i) privacy law in Canada is still relatively new and accordingly remains in flux; and (ii) the employer/employee relationship is founded on a natural power imbalance. In this context, it is not entirely clear which interests will prevail. Consultation processes with respect to the application and scope of such legislation continue to occur. Accordingly, it is plausible that the various government offices which oversee Canada’s privacy laws will eventually redefine matters over which they have jurisdiction, and strengthen the breadth and effect of Canadian Privacy Legislation over time. The Office of the Privacy Commissioner of Canada is currently leading a consultation process to improve and strengthen PIPEDA. Among the current recommendations that have been posed is the possibility of adding a specific provision to PIPEDA to deal with consent issues relating to employees. With this in mind, it is advisable that counsel ensure that their clients conduct their privacy practices in a manner that are relatively consistent with recommendations posed by the Office of the Privacy Commissioner of Canada and its provincial counterparts. Given the uncertainty that surrounds Canada’s current privacy landscape, this is perhaps the most counsel can do to ensure that their clients are privacy-compliant.
For more information on this topic, or any other legal topic relating to corporate, privacy or technology law, please do not hesitate to contact the author, Candice Teitlebaum, at 416.865.4743 or cteitlebaum@airdberlis.com.

Candice Teitlebaum is an associate at Aird & Berlis LLP and belongs to its Corporate/Commercial law group and Technology Industry Team.

1 This article focuses primarily on the impact of PIPEDA on the cross-border transfer of employee data and discusses briefly the impact of British Columbia’s Personal Information Protection Act, S.B.C. 2003 c. 63 (“B.C. PIPA”); Alberta’s Personal Information Protection Act, S.A. 2003, c. P-6.5 (“Alberta PIPA”); and Quebec’s the Act respecting the protection of personal information in the private sector, R.S.Q., c. P-39.1 (“Quebec Act”).

2 Organizations subject to the private sector privacy legislation in Alberta, British Columbia and Quebec are intended to remain subject to PIPEDA in respect of any disclosure of personal information outside the province.

3 Pursuant to ss.2(1) of PIPEDA, “Personal Information” means information, recorded or otherwise, about an identifiable individual, with the exception of the name, title, business address, or business telephone number of an employee of an organization. “Personal Employee Information” under Alberta’s PIPA simply means personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating an employment relationship. The definition of Employee Personal Information under B.C.’s PIPA is similar.

4 PIPEDA governs the collection, use and disclosure of personal information, including employee information, in the context of the transfer of personal information across provincial or national borders only if the information is transferred in the course of a commercial activity. “Commercial Activity” under PIPEDA is defined as any particular transaction, act or conduct or any regular course of conduct that is of a commercial character. Case law indicates that, in its ordinary meaning, “commercial activities” refer to purposes related to trade and the buying and selling of commodities. Arguably, the transfer of employee data for the purpose of administering an employer/employee relationship does not appear to constitute commercial activity, as such is defined pursuant to PIPEDA.

5 If an organization carries on a “federal work, undertaking or business” only then will PIPEDA apply in respect of the personal information of its employees that it collects, uses or discloses (a.4(1)(b)).

6 When contacted via telephone, the Office of the Privacy Commissioner of Canada has noted that it is unlikely that it would have jurisdiction to hear a complaint commenced by an individual opposing the transfer of employee information outside Canada. Similarly, the Office of the Information and Privacy Commissioner for British Columbia and the Office of the Information and Privacy Commissioner of Alberta have noted that they do not have jurisdiction when the personal information of their employees is transferred outside their respective provinces. The issue of jurisdiction pursuant to Canadian Privacy Legislation remains unclear and inconsistent. This is one issue to which counsel should pay attention as consultation processes with respect to the scope and application of Canadian Privacy Legislation ensue.

7 Albert PIPA and B.C. PIPA uphold a reasonable person standard with respect to the collection, use and disclosure of employee information.

8 See Findings of the Office of the Privacy Commissioner of Canada in “Commissioner’s Findings – PIPEDA Case Summary #313: Bank’s Notification to Customers Triggers Patriot Act Concerns”, online at http://www.privcom.gc.ca/ef-dc/2005/313_20051019_e.asp. For example, the personal information of Canadians transferred to the United States is impacted by the U.S.A. Patriot Act.

9 Ibid. In this instance, the third-party’s security policy included “administrative, technical and physical protections to safeguard against, inter alia, unauthorized usage, modification, copying, accessing or other unauthorized processing”.