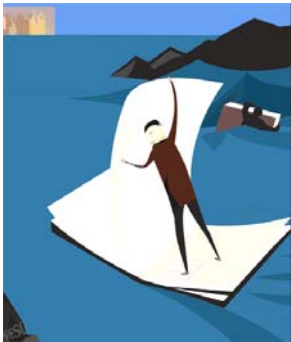


Singleton Urquhart LLP
1200 – 925 West Georgia Street
Vancouver, BC V6C 3L2
T 604. 682 7474
F 604. 682 1283
su@singleton.com
www.singleton.com



BARBARA CORNISH

IMPLEMENTING PIPA IN THE WORKPLACE

IMPLEMENTING PIPA IN THE WORKPLACE

Barbara Cornish

A consideration of employment issues which may arise under the new *Personal Information Protection Act*, (referred to herein as "PIPA" or the "Act"), is important for a number of reasons. First, most day to day functions of an organization are carried out by employees. To the extent that the Act requires an organization to develop and follow practices and procedures to ensure compliance with the Act, the day to day implementation of those practices and procedures will likely fall to its employees. Education and training of employees in privacy matters is therefore essential in order for an organization to properly meet its responsibilities under the Act.

Second, the failure of an employee to adhere to an organization's privacy policies and procedures can have serious consequences for the organization in the form of adverse publicity, time, expense, fines, and in serious cases, civil damages (ss. 56 and 57). As such, the implementation of privacy policies in the workplace raises issues of employee performance and competence which could potentially expose the organization to significant liability. As in all other issues of employee performance, it is essential, therefore, that an organization have internal procedures to monitor and ensure employee compliance with the standards set out in the applicable privacy policy. Indeed, organizations may choose to make adherence to privacy practices and procedures a term and condition of employment, such that repeated, deliberate, or otherwise culpable breaches of those terms and conditions may result in the imposition of disciplinary measures.

While non-compliance with an employer's policies and procedures can often be justified as conduct which may attract disciplinary measures, the law generally requires that the policies be clearly articulated, and that an employee be fully cognizant of the standard of performance expected. It is only then that a breach of that standard can result in discipline. The "bottom line" is that it makes sense, both from a liability and a human resources perspective, to inform, educate and train all employees in their privacy obligations.

Third, unlike the Federal Act, PIPA and its Alberta counterpart, specifically include employee personal information under the definition of "personal information". Thus, employee personal information is now subject to the same level of protection as any other type of personal information. As well, employees now have the right to access and, if appropriate, correct the accuracy of their personal information in the custody and control of the organization. Organizations who do not deal in personal information in the course of their day to day business will therefore nevertheless have significant responsibilities under the Act with

respect to their collection, use and disclosure of employee personal information. In recognition of these responsibilities, I encourage employers with any significant number of employees to develop and implement a separate employee privacy policy.

EMPLOYEE PERSONAL INFORMATION

The Act provides a broad definition of "personal information" as follows:

"personal information" means information about an identifiable individual and includes employee personal information but does not include:

- (a) contact information, or
- (b) work product information.

Personal information will include information such as, but not limited to:

- (1) residential information;
- (2) age, income, marital status, dependents and ethnic origin;
- (3) social insurance number, driver's licence number, credit card number and bank account information;
- (4) employment application forms, resumés, reference letters and transcripts;
- (5) employee information such as compensation, evaluations and assessments, management opinions of employees and disciplinary actions;
- (6) office devices which record entry and exit times and video surveillance;
- (7) DNA and fingerprint samples;
- (8) Photographs;

- (9) internet activity and other computer monitoring;
- (10) leisure activities or hobbies; and
- (11) personal preferences of the individual.

"Employee personal information" is defined as:

Personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment.

SECTIONS 13, 16 & 19 - COLLECTION, USE AND DISCLOSURE OF EMPLOYEE PERSONAL INFORMATION

The collection, use and disclosure of employee personal information is regulated pursuant to ss. 13, 16, and 19 of the *Act* respectively.

Section 13 provides:

- "13**
- (1) Subject to subsection (2), an organization may collect employee personal information without the consent of the individual.
 - (2) An organization may not collect employee personal information without the consent of the individual unless
 - (a) section 12 allows the collection of the employee personal information without consent, or
 - (b) the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.
 - (3) An organization must notify an individual that it will be collecting employee personal information about the individual and the purposes for the collection before the organization collects the employee personal information without the consent of the individual.

- (4) Subsection (3) does not apply to employee personal information if section 12 allows it to be collected without the consent of the individual.

THE REQUIREMENT OF NOTIFICATION

It is significant to note that while the *Act* dispenses with consent in relation to the reasonable collection of employee personal information for the purpose of establishing, managing or terminating the employment relationship, s. 13(3) nevertheless requires the organization to notify the employee that it will be collecting the information for the purposes of that collection.

This requirement of notification is unique to employee personal information and applies to all information collected after January 1, 2004, when the *Act* came into force. (s. 3(2)(i))

Sections 16 and 19, which respectively govern the use and disclosure of employee personal information, also dispense with consent with respect to the purposes of establishing, managing, or terminating the employment relationship. A similar notification requirement to s. 13 is also provided in those sections.

"REASONABLE" COLLECTION, USE AND DISCLOSURE

Consistent with other provisions of the *Act*, PIPA does not specify what type of information may be collected, used or disclosed without the employee's consent. Rather, it imports a reasonable purpose standard.

The collection, use and disclosure of the following "typical" employee information would, in my view, likely be considered reasonable:

(a) **Establishing an employment relationship**

- | | |
|-----------------------|-----------------------|
| - resumés | - benefit enrollment |
| - job application | - payroll data |
| - reference inquiries | - banking information |

(b) Managing an employment relationship

- benefit information
- payroll data
- banking information
- benefit applications
- RRSP/pension contribution
- emergency control information
- performance appraisals/pay increases
- discipline notes
- health/illness/absenteeism
- accommodation requests
- WCB information
- garnishment orders

(c) Terminating an employment relationship

- benefit/pension information
- severance information
- letters of resignation
- reference requests
- performance appraisals
- discipline notes
- health/illness/absenteeism
- WCB/UI/tax/Employment
Standards information

THE RETENTION OF EMPLOYEE PERSONAL INFORMATION

Section 35 provides for the retention of personal information including employee personal information. It provides:

- "35 (1) Despite subsection (2), if an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

- (2) An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that
 - (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and
 - (b) retention is no longer necessary for legal or business purposes."

The reference to the retention of employee information for "legal or business purposes" in s. 35(2) incorporates the requirements of retaining certain employee records pursuant to the *Employment Standards Act* for 2 years after the employee departs from the organization and for 6 years pursuant to the *Income Tax Act*. Note that it may not be considered a necessary business or legal purpose to maintain all employee information for this long.

Section 35(2) has application to individuals who apply to organizations for employment and in the course of doing so supply personal information, often in the form of a resumé. If that information is used to make a decision to hire or not hire the individual, it must be retained for a year after that decision is made.

PROTECTION OF EMPLOYEE PERSONAL INFORMATION

Pursuant to s. 34 of the *Act*, an organization is required to make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, or disposal of personal information, including employee personal information.

In practice, such security measures would generally include providing access to employee personal information on a strictly "need to know" basis. Health and financial information are typically amongst the most sensitive of personal information, but are routinely collected, used and disclosed in the normal course of employee relations. Security measures must, therefore, be used to protect this information. Such measures may include, at the very least, locking filing cabinets, restricting computer access, and shredding document copies.

DISCLOSURE OF EMPLOYEE PERSONAL INFORMATION TO THIRD PARTIES

It is important to note that s. 34 refers to the protection of personal information under an organization's "custody" or "control". The former generally connotes physical possession, while the latter does not.

Organizations typically have "control" but not always "custody" of a wide variety of employee personal information, which is sent to third parties. Most organizations send information to government bodies such as Employment Insurance, Income Tax, WCB, etc. Similarly, employee personal information is often sent to benefit providers. In many organizations, payroll or other activities such as benefit administration may be outsourced to third parties. Before providing this information to third parties the employer-organization must consider the use of reasonable security arrangements (often in the form of indemnities or third party contracts/undertakings) to ensure a reasonable level of protection. Many of you may have already received similar contracts from these third parties.

ACCESS TO AND CORRECTION OF EMPLOYEE PERSONAL INFORMATION

Parts 7 and 8 of the *Act* (ss. 23-32) provide employees with the right to access their personal information and to request correction of any inaccuracies. The fact that a response to such a request must (subject to requests for an extension of time) be provided within 30 days (s.29), may impose significant time pressures on organizations who are not adequately prepared and may not know where to locate all of the information requested.

OWNERSHIP OF PERSONNEL FILES

Prior to the enactment of PIPA, many labour and employment specialists were of the opinion that the employer owned the human resources and personnel files. With the advent of PIPA, this is likely no longer the case.

SHADOW FILES

Similarly, in many large organizations, ad-hoc personnel files, investigation files or other secondary human resources files - commonly known as "shadow files" were generated, often by the direct supervisor of the employee. Those days are now likely over, particularly if an employer wishes to make a decision on information maintained in the shadow file, it will likely be subject to PIPA obligations.

REFERENCE CHECKS

The enactment of PIPA will require employers to obtain an employee's consent to provide references or other employee personal information to third parties after the employee has left the employ of the organization.

MISCELLANEOUS ISSUES

This paper has attempted to address some of the basic issues which will confront employers subject to the requirements of PIPA. Other topics relevant to the employment context include the following issues which have not yet been fully resolved.

Jurisdictional issues - what legislation applies?

If an employer carries on business solely in British Columbia, then the matter is relatively straightforward. So long as the activity is not a federal undertaking (i.e., banking, inter-provincial trucking, etc.) then PIPA applies. Conversely, if the employer is a federally regulated employer, such as an inter-provincial trucking company, then the federal legislation applies. The more complicated issue arises when a corporate head office, often housing the Human Resources Department, is located in one province, for example, British Columbia, but employees are working in other provinces. Which legislation applies? If the two provinces are B.C. and Alberta, the issue is less complicated given the efforts of these provinces to work together to establish fairly similar legislation. What happens if the employer has branch operations in Saskatchewan? (Saskatchewan, choosing not to enact its own legislation is by default governed by federal privacy legislation). Does the employer have to maintain employee personal information pursuant to the standards of PIPA (location of head office) or pursuant to Saskatchewan (federal legislation) where the employee actually works?

Other employers may have head offices or corporate Human Resource Departments in the United States. Because employee personal information has crossed the international border, will the employer have to comply with federal legislation in addition to PIPA, or only the federal privacy legislation? Does federal privacy legislation, even if applicable, apply to personal employee information used within the same employer organization?

The federal privacy legislation defines personal information as being personal information that an employer discloses across borders for a "commercial purpose." It is not clear whether cross-border, intra-corporate collection, use or disclosure of employee personal information would be considered a "commercial purpose" within the meaning of that Act.

The application of PIPA to the unionized workplace

The unionized workplace is a unique tripartite arrangement involving not only the employer and employees, but also the Union, which functions as the exclusive bargaining agent on behalf of all employees. In the unionized workplace, there are no individual employee contracts. Rather, the Union enters into a single contract (the Collective Agreement) with the employer on behalf of all employees.

Typically, unions and management of the company will discuss employment matters including, often, personal information relating to individual employees, in the expectation that such communication will not necessarily be divulged to the employee(s) in question. Unions are now specifically included in the definition of "organization" under the Act, with the result that they too will be required to not only safeguard employee personal information, but provide access to that information on request by an employee. The upshot is that employers will now have to be far more cautious in dealings with all third parties - including Unions. Having said that, recent caselaw has raised the issue of to what extent, if any, the Federal Act, (and presumably therefore, also the Provincial Act) apply in the labour arbitration context. The application of privacy laws to the unionized workplace may therefore be different than the non-unionized workplace. See *L'Écuyer v. Aéroports de Montréal*, [2003] F.C.J. No. 752 (F.C.T.D.) (attached). This issue, like others, remains unclear. Only time will tell how the legislation will be interpreted and administered.