dentons.com

DENTONS

Insights and Commentary from Dentons

On March 31, 2013, three pre-eminent law firms—Salans, Fraser Milner Casgrain, and SNR Denton—combined to form Dentons, a Top 10 global law firm with more than 2,500 lawyers and professionals worldwide.

This document was authored by representatives of one of the founding firms prior to our combination launch, and it continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

PRIVACY LAW AND THE ONTARIO PRIVATE SECTOR EMPLOYEE INFORMATION

June 17, 2003

By Anneli LeGault
Partner
Fraser Milner Casgrain LLP

FRASER MILNER CASGRAIN LLP

TABLE OF CONTENTS

Federal Law

While the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") is a piece of federal legislation, it will affect many provincially regulated organizations as well. The Act comes into effect in three stages.

As of January 1, 2001 it applied to personal information (except for personal health information) that is collected, used or disclosed during the commercial activities of federal businesses. Federally regulated businesses are those that are covered by the *Canada Labour Code* and *Canadian Human Rights Act* and include banks, airlines, inter-provincial transportation, radio and television broadcasting and telecommunications companies. As of 2001, the Act applied as well to personal information about employees that was retained by these federally regulated employers.

Also, as of January 1, 2001, certain provincially regulated organizations were covered by the Act if they exchanged personal information across provincial or national borders for "consideration" - i.e. payment. Examples of such organizations would include credit reporting agencies and organizations which sell or exchange mailing lists.

Since January 1, 2002 the Act has applied to the personal health information collected, used and disclosed by the organizations described above.

As of January 1, 2004 the Act will apply to the collection, use or disclosure of personal information in the course of commercial activities within a province - ***unless*** the federal government exempts the organization in provinces that have adopted substantially similar privacy legislation. To date, only the province of Quebec has passed substantially similar legislation - the *Act Respecting the Protection of Personal Information in the Private Sector* passed in 1994.

Provincial Initiatives

The federal government has confirmed that organizations covered by the Quebec legislation will be exempted from the *Personal Information Protection and Electronic Documents Act*.

As of the time of writing, Alberta and British Columbia have both introduced draft legislation to cover the private sector. However, both Bills have been criticized by the federal Privacy Commissioner as deficient. Ontario's plan to introduce legislation (which was already drafted in 2002) has stalled and it remains uncertain as to whether Ontario will introduce its own legislation.

The big question for human resources managers of provincially regulated companies in provinces other than Quebec is what will happen if the province in which you operate does not pass its own equivalent legislation. PIPEDA will not apply to human resources matters - personnel files, payroll records, benefit forms, grievance files, workers' compensation reports and the like. However, it can apply to commercial use of employee information, such as producing a marketing brochure. As well it will apply to non-employees who are providing services such as consultants and independent contractors. Many employers are putting personal information protection processes into place to meet employee concerns, to be in compliance with

any provincial legislation which is passed, and to ensure consistency in the company's practices across the country.

Canada's Privacy Legislation: The Basics

There are four basic principles underlying Canada's personal information protection legal regime: consent, defining purposes, security, and access.

PIPEDA is based on the principle that an organization requires an individual's ***consent*** to collect, use or disclose personal information about that individual. The organization must also tell the individual what the ***purpose*** of the collection, use or disclosure will be. The personal information must be stored in a ***secure*** manner and the individual is entitled to ***access*** any and all personal information being held about him/her.

Personal information is not exhaustively defined in the Act. The Act states that personal information means "information about an identifiable individual", excluding the name, title, business address and business telephone number of an employee. The exclusion from the definition, therefore, allows an employer to continue to publish and issue personnel directories, business cards, phone listings and advertising materials which include employee contact information. As well, if personal data has been rendered anonymous (such as salary ranges without names, or the results of an employment equity survey), it is no longer personal information covered by the Act.

Examples of personal information of relevance to human resources management include: payroll records, employee home telephone numbers and addresses, Social Insurance Numbers, performance appraisals, discipline records, grievance forms and files, names of beneficiaries and dependents, date of birth, doctor's notes, identification numbers, pension and benefit application forms.

The Ten Privacy Principles

The *Personal Information Protection and Electronic Documents Act* (and any similar provincial legislation which is passed) incorporates ten principles. The ten privacy principles are:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

This paper outlines the ten privacy principles and provides examples from human resources management to illustrate the application of the Act.

1. Accountability

Organizations are responsible for the personal information under their control.

Requirements:

- company must designate someone to be in charge of the company's compliance with the privacy legislation
- company must have policies and procedures in place to comply with the privacy legislation
- company must protect all personal information held by the company or sent outside for any reason, including processing

Human Resources Examples:

- appoint a Privacy Officer
- communicate the identity of the Privacy Officer
- develop policies and procedures to cover employees' personal information (which would include the information relating to former employees, contractors and temporary staff from outside agencies)
- communicate the policies
- analyse current personal information handling practices to see what you have, how it is collected and stored, why it is collected, when it is disclosed, how it is retained, when and how it is destroyed
- review your practices with respect to sending information outside for processing, translation, printing, storage, to a payroll service provider, bank, or pension administrator
- review the personal information protection handling practices of the outside agency or ensure through your contractual arrangements that they will certify that they are privacy compliant

2. Identifying Purposes

Organizations must advise individuals why they are collecting the personal information at or before the time of collection.

Requirements:

- identify the purpose of collecting the information
- inform the individual of the purpose

- this notification can be done orally or in writing, depending upon the sensitivity of the information

Human Resources Examples:

- inform a job applicant in a statement on the application form as to why you are collecting the information on the form
- after hiring an individual you may orally tell the employee why you need an emergency contact name and number
- inform the employee that you require their bank account information to arrange for direct deposit of their pay
- inform the individual that you need their Social Insurance Number to make contributions to Canada Customs and Revenue Agency for income tax, Canada Pension Plan and Employment Insurance
- on the benefit application form or on the computer screen for your electronic enrolment inform individuals that you are collecting the information in order to administer the benefit plan and provide benefits

3. Consent

Organizations are required to obtain an individual's consent to collect, use or disclose personal information. Consent may be implied or expressly granted.

Requirements:

- obtain consent from the individual whose personal information is collected, used or disclosed
- this is usually done at the time of collection
- this can be done in a written or oral format, depending upon the sensitivity of the information
- keep a record of the consent

Human Resources Examples:

- tell current staff what you have on file currently, what you use it for, where and why you disclose it and allow the employees an option to withdraw their consent to ongoing use and disclosure
- obtain express consent for the use of sensitive information such as Social Insurance Number and health information

- you may use implied consent in situations such as the following: where the employee gave the employer their home address for mailing this year's award, you may assume that it is acceptable to send next year's award to them as well, unless informed otherwise

- you may want to use a check-off box for less sensitive information - e.g. "if an employee does not want the company to pass on their name to the United Way Campaign, for example, check here"

4. Limiting Collection

Organizations are only entitled to collect the personal information necessary to fulfil the stated goals.

Requirements:

- once the purpose has been identified, the company must limit collection to what is truly necessary to fulfil that purpose

Human Resources Examples:

- do not collect the name of an elementary school on an employment application form

- do not collect information about driving records or driving licenses, unless the position requires driving as a regular job duty

- on a pension application form you may require date of hire, date of birth, marital status, identity of spouse, but not the individual's medical history

5. Limiting Use, Disclosure and Retention

Personal information must be used or disclosed only for the purposes for which it was collected, except with the individual's consent or as required by law.

Requirements:

- do not use or disclose the personal information for other purposes, unless you receive consent or this has been required by law

- a new use or a new disclosure will require a new consent

- keep the information only as long as necessary to fulfil the original purpose

Human Resources Examples:

- if the photograph of an employee in the personnel file is obtained for security reasons, do not include it in advertising brochures for the company

- if the Social Insurance Number was collected for payroll administration, do not use it as an employee identifier or for the benefit plan (this would be a breach of the *Income Tax Act*, in any event)

- check your provincial labour standards legislation or the *Canada Labour Code* (if federally regulated) for how long certain payroll records need to be kept (this is usually three years)

- Canada Pension Plan, Employment Insurance and income tax information should be kept for six years after the year to which they relate

- you may wish to keep interview notes of unsuccessful candidates for the six to twelve-month limitation period provided by your applicable human rights legislation, in the event of a human rights complaint being filed

- after that time, you should dispose of all interview notes and application forms, unless the individual has consented to their retention in the event of future openings

- you would not need to keep garnishment records after the garnishment has been completed (retaining the records may influence a supervisor on a future promotion or transfer decision)

- develop retention guidelines

- develop procedures for destroying personal information (for example, shredding), erasing electronic records or making records anonymous

6. Accuracy

The information must be kept as accurate and as current as necessary to fulfil the stated purposes.

Requirements:

- personal information must be as accurate, complete and up-to-date as necessary for the purposes for which it is used

- update personal information when necessary to fulfil the specific purposes

- the degree of updating depends upon the use made of the information

Human Resources Examples:

- routinely keep accurate information about salary, bank account, dependents and home address
- you may put the onus on employees to update personal information in their knowledge such as home telephone number, home address and bank account information

7. Safeguards

Companies must protect the personal information by security safeguards appropriate to the sensitivity of the information.

Requirements:

- the company must protect personal information against loss and theft
- the information must also be protected against unauthorized disclosure, copying, use or alteration
- the degree of security depends upon the sensitivity of the information
- types of safeguards include the following: physical measures; organizational measures; and technological measures
- employees who handle the personal information must be trained with respect to the importance of maintaining confidentiality; after all, you are only as strong as your weakest link
- provide training to all human resources, benefits and payroll staff
- set up secure methods for disposal and destruction of personal information which is no longer being retained

Human Resources Examples:

- train all staff who handle payroll, personnel files, medical records, pension and benefits information, recruiting, health and safety, workers' compensation, and training records about the confidentiality procedures; this includes a ban on "gossiping" where someone may be overheard
- shred human resources employee information rather than throw it in the garbage
- use a courier or other secure method to provide information to your payroll service provider, pension administrator and benefit plan administrator

- conduct regular internal security audits
- change passwords on a regular basis
- determine what a supervisor can view with respect to any direct or indirect reports
- keep medical and workers' compensation records and reports separate from the personnel file which is viewed by a manager
- do not send personal information out of the company as an e-mail attachment
- make sure that employees in human resources follow procedures with respect to storage of work in progress at the end of the day, over lunch and over breaks so that documents are not left on a desk
- physical measures in the human resources department can include locked filing cabinets, and restricted access to the human resources offices
- organizational measures would include security clearances, limiting access on a "need to know" basis, staff training and agreements with your external service providers which include their privacy guarantees
- technological measures include use of passwords and encryption, fire walls and separating identifiers from sensitive data

8. Openness

Companies must provide specific information about their personal information management policies and practices.

Requirements:

- the company must inform individuals about the personal information it holds, the purposes for which it is used, to whom it is disclosed and how the individual can access the information
- the company must make information easily available about its personal information management policies and procedures
- this can be done online or by way of a brochure, policy manual or employee handbook
- the company must make available the following information:

  (i) the name and address of the company's Privacy Officer

  (ii) how an employee can access his or her own personal information

(iii) a description of the type of personal information held at the company and a general accounting of its use

(iv) any brochures or other information that describe the privacy policy

(v) what information is shared with a related organization, such as an affiliate or subsidiary

Human Resources Examples:

- this information sharing can be online, in a brochure, policy manual or employee handbook
- train human resources staff to be able to answer questions about personal information protection
- include the identity and contact information for the company's Privacy Officer in any employee handbook, policy manual or company Intranet
- include information about how to access personnel files in any employee handbook, policy manual or company Intranet

9. Individual Access

Individuals are entitled to have access to their personal information retained by organizations and are entitled to information about the use and disclosure of their information.

Requirements:

- individuals can request access to personal information held about them
- individuals have the right to receive copies of the personal information
- the company must correct or amend personal information if the accuracy or completeness is justifiably challenged
- access must be given by the company at minimal or no cost
- the company must provide reasons for any refusal; justifiable reasons include solicitor-client privilege, litigation privilege, security and ongoing fraud investigations, proprietary or trade secret information, references to other individuals, sensitive medical information (this can be made available through a medical practitioner), prohibitively costly to provide (for example, request for 20 years of payroll records), information provided during a formal dispute resolution process such as alternative dispute resolution or mediation, or providing the information could reasonably be expected to threaten the life or security of another individual

Human Resources Examples:

- the human resources department should organize and consolidate employee data banks
- remember that access does not apply just to current staff, but anyone who has personal information being retained by the company can request access to that information, including unsuccessful job candidates, former employees, dependents and beneficiaries of employees, staff of temporary service agencies, consultants or contractors
- prepare a form for access requests
- have a form letter ready for responding to a request which includes the time limits by which the company is bound (the federal legislation requires 30 days to respond to an access request, but this can be extended for a further 30 days in certain circumstances)
- have a form letter ready for overly broad requests
- tell individuals of the use made of the information and of third parties to whom it is disclosed
- train supervisors on how to keep their own notes and address the "shadow file" situation (supervisors frequently keep their own notes outside of the human resources files, and as these are company property, they could be accessed by individuals as well)
- remember that personal information is not only kept in the personnel file; it could include information in payroll, benefits, health services, training, recruitment or even accounting (for example, expense forms submitted by the individual)

10. Challenging Compliance

Individuals have the right to file a challenge about the company's compliance with the company's Privacy Officer.

Requirements:

- put in place a complaints procedure and an inquiries process
- investigate all complaints and notify individuals of the outcome
- correct any inaccurate personal information or modify procedures in response to a justified complaint
- keep records of complaints and responses

Human Resources Examples:

- describe your complaint process in your employee handbook, policy manual or company Intranet

- employees of federally regulated employers can also complain to the Privacy Commissioner of Canada. As well, Quebec has the Commission d'access à l'information. Most complaints filed before the Commission have involved a refusal of access.

As various provinces pass their own equivalent legislation, they will likely set up government bureaucracies to which employees can complain if they think their own employer is not in compliance with the legislation or with its own policies and procedures.

June 2003
Anneli LeGault
Fraser Milner Casgrain LLP