Protecting Your Employee’s Privacy in 2016

It seems that more and more people have accepted having less and less privacy. Yet as an organization you are required to ensure you are taking adequate steps to ensure the privacy of the information you gather and maintain about your employees.

Consider for a moment all the information you are routinely gathering about your employees. What would that list contain?

1. **During Recruitment and Hiring** you gather
   - Resumes, application forms, interview notes, background and criminal record checks and pre-employment tests
   - Upon hiring you record information such as Social Insurance Numbers, Canada Revenue Agency forms, application for benefit forms, which includes information such as date of birth, names of family and
2. **While employed you gather information such as**
   - **Compensation:** salaries, bonuses and commissions, payroll records, bank account information
   - **Performance:** performance evaluation scores, discipline records including warning letters, evidence collected during investigations into employee misconduct and investigation findings
   - **Employee monitoring:** security entry information that may include biometrics, images, video surveillance records and even GPS tracking records
   - **Medical and Health information:** doctor’s notes, medical records provided for the purpose of obtaining sick leave or disability benefits, requesting accommodation of a disability, or upon a return to work following an illness or injury
3. **At Termination:**

- Termination letters, severance agreements, letters of employment, references

4. **Miscellaneous Information**

- You may also track email records, records of calls, Internet usage and information stored on computer networks accessed by your employees.

Some of this information will be subject to privacy laws, which means you have to ensure you are keeping it safe, storing, using and deleting it according to privacy legislation or laws in your jurisdiction.

In Canada there are Federal and, in some places, Provincial privacy Laws in place you will need to consider:

- **Federal**: The *Personal Information Protection and Electronic Documents Act* (**"PIPEDA"**)
- **Alberta:** The *Personal Information Protection Act* (**"Alberta PIPA"**)
- **British Columbia:** The *Personal Information Protection Act* (**"BC PIPA"**)
- **Quebec:** *An Act respecting the protection of personal information in the privacy sector* (**"Quebec Private Sector Act"**)
- **Manitoba:** *The Personal Information Protection and Identity Theft Prevention Act* (**"PIPITPA"**)

The remaining Provinces and Territories rely on PIPEDA for private sector employers and a variety of local legislation to govern public sector employers.

5 Privacy Policy Components

It is useful to put in place privacy policies that apply specifically to the protection of your employee's information. Information that falls into the wrong hands can spell problems for your organization if you failed to ensure the information was properly managed and secured. If one of your employees accidently or purposely sends information about another one of your employees out across the Internet or if third parties do not properly secure information you provide them, you may find yourself facing penalties and fines. To begin go mitigate potential problems ensure your policies cover all your bases. Consider these components of your organizations privacy policies:

1. ***What Information will your Policy Cover***

- Identify the information you are collecting and need to collect, and determine what is personal and what is not (i.e. business information such as job title, work email) and what you need to keep and what you do not.

2. ***Identify the Purpose and Process for Collection, Use and Disclosure***

- Determine the purpose for the information and how you are using it
- Determine if you are sharing that information with third parties (i.e. benefits administrator, payment service) and the location of the third parties (within Canada, outside of Canada) and determine if the legislation in your jurisdiction is being applied

3. ***Determine how are you ensuring security of the information***

- Are you storing the information, if yes, how and where?
- Identify the steps you are taking to ensure protection of personal

information
- Identify who has access to the personal information and ensure they are trained and compliant in privacy requirements

4. ***Identify the process for retention and removal of the information***

   - Length of time you are retaining the personal information
   - Method of ensuring the information is disposed when no longer needed (this would include information stored on back up servers including third party servers and in the cloud).

5. ***Employee Access and Updating***

   - Method (including contact person and process) to enable employees to access, review, verify and update their information

Creating policies and training all employees on the proper gathering, storage and access to private information is a vital activity in today's workplace. Your employees are often sharing information quickly and easily, submitting expenses electronically, being paid directly into bank accounts, sending personal emails through company servers and more. Draft clear, comprehensive privacy policies and take steps to inform and train all of your staff on the importance of protecting private information.