BACK TO DATAGUIDANCE

DataGuidance GUIDANCE NOTES

About The Author

Lyndsay Wasser is a Partner at McMillan LLP, Co-Chair of McMillan's Privacy Group and a Certified Information Privacy Professional/Canada. Lyndsay advises and assists management in all areas of employment, labour, pension and benefits laws, including advising on hiring, performance management, employment standards, human rights laws and employment terminations, as well as drafting or reviewing employment contracts, compensation plans and employment policies.
Lyndsay also regularly advises and assists clients on a broad range of privacy issues, including advising on access requests, privacy breaches, workplace privacy issues, e.g., background checks, computer/video/phone monitoring, GPS tracking, drug and alcohol testing, handling personal health information, and transferring personal information across borders, as well as helping organizations to develop privacy compliance programs, privacy and social media policies, data sharing agreements and consent forms. Lyndsay regularly writes and speaks on privacy-related topics, and is the co-author of Privacy in the Workplace, Third ed. and the Privacy chapter in the Ultimate Corporate Counsel Guide.
Lyndsay also regularly provides advice and assistance to vendors and purchasers with respect to the employment and privacy aspects of corporate transactions, including negotiating the employment and privacy terms of purchase agreements, evaluating employment issues in the transaction, and drafting offer letters and other contracts for transferring employees.
Email: lyndsay.wasser@mcmillan.ca

Canada - Employment

Lyndsay Wasser

12 May 2017

1. Introduction and Overview

1.1 Key acts, regulations, directives, guidelines, noteworthy decisions, and case law

1.1.1 General Legislation

Protection of employee personal information in Canada varies across jurisdictions. The following legislation applies to private sector employers ('Canadian Privacy Legislation[1]'):

- The Personal Information Protection and Electronic Documents Act, SC 2000, c 5 ('PIPEDA'), governs the collection, use, disclosure and protection of employee personal information by federally regulated employers, e.g., banks, inter-provincial transportation, telecommunications, shipping and aerospace;
- The Personal Information Protection Act, SA 2003, c P-6.5 ('Alberta PIPA'), governs the collection, use, disclosure and protection of employee personal information by provincially regulated employers in Alberta;
- The Personal Information Protection Act, SBC 2003, c 63 ('B.C. PIPA'), governs the collection, use, disclosure and protection of employee personal information by provincially regulated employers in British Columbia;
- An Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 (the 'Quebec Act') governs the collection, use, disclosure and protection of employee personal information by provincially regulated employers in Quebec.

In addition to the above, Manitoba has passed The Personal Information Protection and Identity Theft Prevention Act, which will apply to employee personal information in Manitoba. However this legislation is not yet in force, as of May 2017.

1.1.2 Employment Legislation

There is no legislation directly applicable to protection of employee personal information by private-sector organisations in any other Canadian provinces. However, there are statutory and common law torts that could apply to breaches of employee privacy by employers, as follows:

1.1.2.1 Statutory Torts

Statutory Torts - British Columbia, Manitoba, Newfoundland & Labrador and Saskatchewan have each enacted a 'Privacy Act', which creates a statutory privacy tort, as follows:

- British Columbia - *Privacy Act*, RSBC 1996, c 373 at s. 1(1) provides that 'it is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.'
- Manitoba - *The Privacy Act*, CCSM c P125 at s. 2 provides that 'A person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person. An action for violation of privacy may be brought without proof of damage.'
- Newfoundland & Labrador - *Privacy Act*, RSNL 1990, c P-22 at s. 3(1) provides that 'it is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of an individual.'
- Saskatchewan - *The Privacy Act*, RSS 1978, c P-24 at s. 2 provides that 'it is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person.'

1.1.2.1 Common Law Torts

Additionally, common law privacy torts have been developed in the following cases:

- Intrusion upon seclusion – In the seminal case of *Jones v. Tsige*, 2012 ONCA 32 (CanLII), the Ontario Court of Appeal recognised a tort whereby: 'One who intentionally intrudes, physically or otherwise, upon the seclusion of another or [their] private affairs or concerns, is subject to liability to the other for invasion of [their] privacy, if the invasion would be highly offensive to a reasonable person[2].' This tort has been alleged, and could potentially apply to privacy breaches by an employer, including highly invasive employee monitoring.
- Public Disclosure of Private Facts – In the seminal case of *Jane Doe 464533 v ND*, 2016 ONSC 541, the Ontario Superior Court of Justice recognised a tort whereby 'One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicised or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public[3].' This tort could potentially apply to unauthorised disclosure of sensitive employee personal information by an employer.

1.1.3 Additional Legislation in Quebec

Quebec also has some additional laws that can be applicable to employee privacy and data protection in certain situations, including:

1. Charter of Human Rights and Freedoms, CQLR c C-12:
   - Section 5 provides that 'every person has a right to respect for [their] private life.'
   - Section 46 provides that 'every person who works has a right, in accordance with the law, to fair and reasonable conditions of employment which have proper regard for [their] health, safety and physical well-being.
2. An Act to Establish a Legal Framework for Information Technology, CQLR c C-1.1. This legislation contains certain provisions governing tracking the location of individuals[4], collection and use of biometric information[5] and the security of technology-based documents, which can be applicable to collection, use and disclosure of employee personal information in some situations.
3. Civil Code of Québec, CQLR c CCQ-1991:
   - Section 35 provides that 'Every person has a right to the respect of [their] reputation and privacy. The privacy of a person may not be invaded without the consent of the person or without the invasion being authorised by law.'
   - Section 36 provides that 'The following acts, in particular, may be considered as invasions of the privacy of a person: (1) entering or taking anything in [their] dwelling; (2) intentionally intercepting or using [their] private communications; (3) appropriating or using [their] image or voice while he is in private premises; (4) keeping [their] private life under observation by any means; (5) using [their] name, image, likeness or voice for a purpose other than the legitimate information of the public; (6) using [their] correspondence, manuscripts or other personal documents.'
   - Section 37 provides that 'every person who establishes a file on another person shall have a serious and legitimate reason for doing so. He may gather only information which is relevant to the stated objective of the file, and may not, without the consent of the person concerned or authorisation by law, communicate such information to third persons or use it for purposes that are inconsistent with the purposes for which the file was established. In addition, he may not, when establishing or using the file, otherwise invade the privacy or injure the reputation of the person concerned.'

In addition, arbitrators frequently recognise privacy rights or interests of unionised employees. Such privacy rights can arise from explicit terms in a collective agreement. In the absence of specific terms in the collective agreement, actions such as drug and alcohol testing, employee monitoring, e.g., video, telephone, computer, GPS, and searches of employees and their property are generally considered to be an exercise of 'management rights' under the collective agreement. Management rights must be exercised reasonably, and arbitrators have developed various tests to assess the reasonableness of employer activities that impact employee privacy.

1.2 Regulators and supervisory authorities

The following regulators have responsibility for monitoring compliance with, and enforcing, the Canadian Privacy Legislation:

- PIPEDA – The Office of the Privacy Commissioner of Canada (the 'OPC');
- Alberta PIPA – The Office of the Information and Privacy Commissioner of Alberta (the 'Alberta Commissioner');
- B.C. PIPA – The Office of the Information and Privacy Commissioner for B.C. (the 'B.C. Commissioner');
- The Quebec Act - The Quebec Commission de l'accès à l'information (the 'CAI').

These regulators publish extensive guidance on compliance with the privacy legislation in their respective jurisdictions. For example, the OPC has published the following resources specifically applicable to employee privacy:

- 'Privacy in the Workplace';
- 'Ten things human resources professionals need to know about privacy;'
- 'Key privacy protection tips for federal human resources professionals;'
- '10 Workplace Tips for Protecting Personal Information on Mobile Devices;'
- 'Privacy and Social Networking in the Workplace;'
- 'Application of the *Personal Information Protection and Electronic Documents Act* to Employee Records';
- 'Privacy in the Time of a Pandemic: Guidance for Organisations.'

The privacy regulators also investigate privacy complaints, and can commence investigations on their own initiative, and frequently publish their decisions online.

2. Recruitment and selection

2.1 Legal framework

An employer's obligations under the Canadian Privacy Legislation apply beginning at the recruitment stage. This includes, without limitation:

- Notice/Consent requirements, including the obligation to notify individuals of the purposes for which their personal information is being collected;
- Reasonableness requirements, including restrictions against collecting more information than is reasonably necessary to evaluate a job candidate's suitability for employment, as well as requirements to limit use, disclosure and retention of the information to only what is reasonable to accomplish the purposes for which it was collected;
- Security requirements, including the obligation to implement physical, technological and

organisational safeguards that are appropriate based upon the sensitivity of the information;
- Accuracy requirements, including taking steps to ensure that information collected is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used;
- Openness requirements – See Section 2.2 below respecting the information that should be available to job candidates;
- Access – Job candidates have the right to access any personal information, broadly defined, that the organisation holds about them, subject to certain limited statutory exceptions as described in Section 4.4 below.

The B.C. Commissioner has published guidelines respecting compliance with B.C. PIPA in the recruitment process, entitled 'PIPA and the Hiring Process.'

In jurisdictions where there is no Canadian Privacy Legislation that is applicable to personal information of job candidates, the above statutory requirements do not apply. However, it is good practice to limit collection, use and disclosure of personal information to only what is reasonable in the circumstances, to avoid allegations of statutory or common law torts.

2.2 Advertising a position

Employers that are advertising for a position should ensure that they provide clear information respecting their personal information handling practices and policies, so that candidates can make an informed decision as to whether they wish to submit their personal information to the organisation. This should include making information available respecting:
- What information will be collected, e.g., if the employer conducts social media checks on applicants;
- How the information will be used, e.g., evaluation for a specific position or evaluation for any positions the employer may have available;
- Who will have access to the information. Note, however, that the Quebec Act specifically requires that individuals be notified of the categories of persons who will have access to their personal information within the organisation;
- Whether their information will be transferred outside Canada. Note, however, that Quebec Act specifically requires notification of the location where the information will be kept, and Alberta PIPA has specific notice and policy requirements if the information will be transferred to, or collected by, a service provider outside Canada, including a corporate affiliate, as described more fully in Section 5.4 below;
- Their rights of access and rectification, including the procedure for exercising such rights. Note, however, that the Quebec Act specifically requires notice of these rights;
- Any choices available to them, e.g., whether they can choose to apply for a specific position versus having their application considered for any opening the employer may have, as well as their right to withdraw their consent if they no longer wish to be considered for employment by the organisation;
- How long their information will be retained if they are not offered employment.

Human rights legislation prohibits discrimination in hiring on the basis of certain characteristics, absent a bona fide job requirement. These vary between jurisdictions but can include: race, colour, sex, pregnancy, sexual orientation, civil status, religion or creed, political convictions, language, ethnic or national origin, place of origin, nationality or citizenship, ancestry, social condition, source of income, mental or physical disability, the use of any means to palliate a handicap, gender identity, gender expression, age, criminal conviction, marital status and/or family status. Reference should be made to the applicable legislation in the relevant jurisdiction to determine which of these apply to the particular circumstances. Although organisations are not strictly prohibited from collecting information on these characteristics, they are prohibited from discriminating against individuals on the basis of them. Collecting such information is not recommended, as it gives rise to the potential that an individual will allege that the information was collected or used for an improper purpose, e.g., as a factor in the decision not to hire the person.

2.3 Obligations of the employer to protect candidate's right to privacy during the interview process

Employers that are subject to Canadian Privacy Legislation have an obligation to protect candidates' privacy before, during and after the interview process, using physical, technological and organisational safeguards. Candidates' information should only be disclosed to persons with a 'need to know' such information for the purpose of evaluating the individual's suitability for employment.

2.4 Employer's right to ask questions/request references

Employers may ask questions respecting job qualification, education and accreditation, work history, e.g., positions held, reasons for leaving prior positions, etc.; experience, e.g., duties performed in prior positions, and information respecting knowledge, skills, abilities; authorisation to work in Canada; and other questions related to matters that are relevant to the position for which the person has applied. Employers should not ask for information that is not reasonably required to evaluate the person's suitability for the relevant position.

No questions should be asked that relate to prohibited grounds of discrimination under applicable human rights legislation, unless strictly necessary due to a bona fide job requirement.

Employers also have the right to request professional references. Listing references on a job application or resume can generally be considered implied consent to contact such references for information relevant to the position for which the individual is being

considered. However, it is generally preferable to obtain explicit consent, e.g., require that the individual indicate on the resume whether the organisation can contact the listed references, and the Quebec Act requires explicit consent.

There is no general requirement for employers to respond to reference requests, and it is generally good practice to obtain evidence that the employee or former employee has consented to disclosure of their personal information to the prospective employer prior to responding to a reference request. However, Alberta PIPA provides, at Section 21(2), that: 'An organisation may disclose personal information about an individual who is a current or former employee of the organisation to a potential or current employer of the individual without the consent of the individual if (a) the personal information that is being disclosed was collected by the organisation as personal employee information, and (b) the disclosure is reasonable for the purpose of assisting that employer to determine the individual's eligibility or suitability for a position with that employer.'

2.5 Candidate's obligation to reveal information

Candidates are not obligated to reveal any personal information about themselves. However, if the information is relevant to the position, the employer may choose not to offer employment to the person if they refuse to provide the information. If the information is not reasonably necessary to evaluate the person's suitability for the position, it should not be requested.

2.6 Retention of information

Pursuant to Canadian Privacy Legislation, employee personal information should only be retained for as long as it is reasonably required to accomplish the purposes for which it was collected. After such time, it should be disposed of in a secure manner.

Under PIPEDA, organisations are required to develop guidelines and implement procedures with respect to retention of personal information, which must include minimum and maximum retention periods.

Employers often retain information of unsuccessful candidates for the time period necessary to protect against any potential legal claims related to the decision not to offer employment to such persons, e.g., an allegation that the reasons for not offering employment related to a prohibited ground of discrimination under applicable human rights legislation. The limitation period for most potential claims is two years, or less, in most jurisdictions, commencing from the time that the individual became aware of the facts giving rise to the claim. Therefore, generally personal information respecting unsuccessful candidates should not retained longer than three years after the candidate is notified that they will not be offered employment, if no claims are made by the candidate against the organisation. However, organisations should determine the limitation period for applicable claims in the relevant jurisdiction(s) and develop an appropriate retention schedule with reference to such laws.

Under B.C. PIPA, personal information must be retained for at least one year if it is used to make a decision about a person. Under PIPEDA, the information must be retained long enough to allow the individual access to the information after the decision has been made.

Furthermore, if an individual has made a request to access their personal information, such information must be retained long enough for the person to exercise their rights under the applicable Canadian Privacy Legislation.

3. Employment records

3.1 Processing of employment records

Under Section 7.3 of PIPEDA, employers can collect, use and disclose employee personal information without consent if: '(a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and (b) the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.'

Under Alberta PIPA and B.C. PIPA, employers can collect, use or disclose employee personal information without consent if: (a) it is reasonable to collect, use or disclose the information for the purpose of establishing, managing or terminating an employment relationship; and (b) the organisation has provided the individual with reasonable advance notification, including notifying the individual of the purposes for which the information will be collected, used or disclosed. Note, however, that under Alberta PIPA the notice requirement only applies to current employees.

Under the Quebec Act, consent is required to process employee personal information, and Section 14 provides that: 'Consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes.' There is no exception to this requirement for employee personal information.

In all other jurisdictions, there are no statutory restrictions upon collecting, using and disclosing employee personal information. However, employers should act reasonably when processing employee personal information, in order to avoid potential tort claims or grievances by unionised employees.

3.2 Notification to the employee

As indicated under Section 3.1 above, advance notice must be provided to employees under PIPEDA, Alberta PIPA and B.C. PIPA in order to collect, use or disclose their personal information without consent. Such notice must describe the purposes for which their personal information will be collected, used or disclosed, as applicable.

Under the Quebec Act, when an employer is establishing a file on an employee, the employer must inform him/her: '(1) of the object of the file; (2) of the use which will be made of the information and the categories of persons who will have access to it within the enterprise; (3) of the place where the file will be kept and of the rights of access and rectification.'

There are no specific notification requirements in other jurisdictions, except as may be contained in a contract, e.g., a requirement in a collective agreement to provide notice of policy changes.

3.3 Retention of employment records

As described more fully under Section 2.6 above, pursuant to Canadian Privacy Legislation, the personal information of employees should only be retained for as long as it is reasonably required. After such time, the organisation should dispose of the information in a secure manner.

The limitation period for most potential claims is two years, or less, in most jurisdictions, commencing from the time that the individual became aware of the facts giving rise to the claim. Therefore, generally personal information respecting employees should not be retained longer than three years after the person's employment terminates, in the absence of any legal claim or access request by the employee. However, organisations should determine the limitation period for applicable claims in the relevant jurisdiction(s) and develop an appropriate retention schedule with reference to such laws.

See Section 2.6 for additional information on the retention of the personal information of employees.

4. Information about workers' health

4.1 General rules on processing of workers' health information and exceptions

The Canadian Privacy Legislation does not differentiate between health information and other types of personal information. Although most jurisdictions have specific legislation applicable to personal health information, such statutes generally only apply to health information custodians or trustees, e.g., doctors, nurses, hospitals, healthcare institutions, etc. Although the health information legislation in some jurisdictions contains some provisions that apply to personal health information that a person receives from a health information custodian or trustee, most of the requirements in such statutes would not apply to employers.

Although the Canadian Privacy Legislation does not contain specific provisions applicable to health information, such information would generally be considered sensitive. Therefore, employers should only collect health information if it is strictly necessary, e.g., to implement appropriate accommodations for a disabled employee, and should collect the minimum information required to accomplish its purposes.

Furthermore, sensitive personal information should be protected by more stringent physical, technological and organisational safeguards. Without limiting the foregoing, health information should be kept in a secure location, apart from the individual's general personnel file, and should only be accessible to a limited number of persons who have a need to know such information to perform their job duties.

4.2 Conditions for legitimate processing

Under the Canadian Privacy Legislation, processing of health information is subject to the same conditions as processing other types of information. Therefore, it can only be processed as needed to accomplish reasonable purposes, and upon obtaining consent or providing notice as described below.

Human rights legislation restricts the amount and type of health information employers can request from employees. Generally employers can collect information respecting functional limitations, as necessary to implement appropriate accommodations, but cannot require information about the person's diagnosis or specific test results. It may be possible to collect additional information if it is reasonably necessary in the circumstances. For example, the employer may be able to request information respecting the side effects of medications, if they could affect job performance or have safety implications. Additional information can potentially be requested, if needed, to evaluate the employee's entitlement to sickness or disability benefits.

4.3 Consent issues

As with other types of employee personal information, under PIPEDA, Alberta PIPA and B.C. PIPA, health information can be collected from the employee without consent upon providing advance notice that the information will be collected and used, including the purposes for which it will be used. Under the Quebec Act, manifest, free and enlightened consent is required to collect any personal information, including health information.

Explicit, written consent is generally required to obtain medical information about an employee from a health information custodian/trustee. Such persons are subject to the health information legislation referenced above, and generally will not disclose any information about a patient without the individual's express consent.

4.4 Employees' rights – to information, access, rectification etc.

In the jurisdictions governed by the Canadian Privacy Legislation, individuals, including employees, have a broad right to access all personal information, broadly defined, held about them, subject to certain statutory exceptions. Although the exceptions vary in different jurisdictions, some common exceptions include if:

- providing access would likely reveal personal information about a third party;

- the employer collected the information in connection with an investigation into a breach of an agreement, including express or implied terms of an employment agreement, or a violation of Canadian law;
- the information is protected by solicitor-client privilege;
- the information would reveal confidential commercial information;
- providing access could reasonably be expected to threaten the life or security of an individual;
- or, the information requested was generated in the course of a formal dispute resolution process.

This list is not all-inclusive, and some exceptions do not apply in all provinces. Furthermore, for some of these exceptions, if the employer can sever the information that falls within the relevant category, that information must be severed and the employee is entitled to access the remaining information. Also, some jurisdictions have additional relevant exceptions to employees' access rights. For example, access can be denied under Alberta PIPA if providing access would reveal the identity of an individual who has provided an opinion about another individual in confidence, and a similar exception to access rights exists under B.C. PIPA.

Employees in other jurisdictions do not have a legal right to access their personal information, absent a contractual right to do so. Such contractual right could potentially arise out of a collective agreement, a written employment agreement or offer letter, or an employment policy.

5. Employees' data transfers

5.1 Legal grounds

Under PIPEDA, Alberta PIPA and B.C. PIPA, employee personal information may be transferred to third parties, including third parties outside Canada, if it is reasonable in connection with establishing, managing or terminating the employment relationship. However, the employer remains responsible for protecting the information, as follows:

- PIPEDA – Schedule 1, s. 4.1.3 provides that 'An organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.'
- Alberta PIPA – Section 5(2) provides that 'for the purposes of this Act, where an organisation engages the services of a person, whether as an agent, by contract or otherwise, the organisation is, with respect to those services, responsible for that person's compliance with this Act.'
- B.C. PIPA – Section 4(2) provides that 'an organisation is responsible for personal information under its control, including personal information that is not in the custody of the organisation.'

Under Section 20 of the Quebec Act, personal information can be transferred to mandataries, agents, or any party to a contract for work or services, without consent, if such third party requires the information to carry out their mandate or contract. However, Section 16 of the Quebec Act contains certain requirements and restrictions related to transferring personal information outside of Quebec, as follows:

'Every person carrying on an enterprise in Québec who communicates personal information outside Québec or entrusts a person outside Québec with the task of holding, using or communicating such information on [their] behalf must first take all reasonable steps to ensure:

(1) that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned, except in cases similar to those described in section 18 and 23;

(2) in the case of nominative lists, that the persons concerned have a valid opportunity to refuse that personal information concerning them be used for purposes of commercial or philanthropic prospection and, if need be, to have such information deleted from the list.

If the person carrying on an enterprise considers that the information referred to in the first paragraph will not receive the protection afforded under subparagraphs 1 and 2, the person must refuse to communicate the information or refuse to entrust a person or a body outside Québec with the task of holding, using or communicating it on behalf of the person carrying on the enterprise.'

In all other jurisdictions, there are no statutory restrictions upon transferring employee personal information to a service provider inside or outside Canada. However, employers should act reasonably when processing employee personal information, in order to avoid potential tort claims or grievances by unionised employees, i.e., only transfer information for reasonable purposes and take steps to prevent misuse of the information.

5.2 Mechanisms for the transfers of data

There are no specific, prescribed mechanisms for organisations to transfer personal information to a third party, whether inside or outside Canada.

Since organisations are responsible for ensuring the continued protection of personal information that is transferred to a third party, as described under Section 5.1 above, organisations typically enter into a data sharing agreement or include privacy and data protection provisions in the service agreement with the third party.

However, in some jurisdictions, it may be possible to transfer the personal information of employees to a corporate affiliate without such contractual protections, if the Canadian

organisation confirms that the affiliate has implemented appropriate privacy policies and practices for the protection of personal information that it processes. The privacy policies and practices of the affiliate should provide a comparable level of protection as compared to the protections the Canadian organisation would implement if it was processing the information itself.

5.3 Sensitive data

Canadian Privacy Legislation does not explicitly differentiate between sensitive information and non-sensitive information, with respect to requirements related to transfers of personal information. However, since sensitive information must be protected by more stringent safeguards, the privacy and data protection provisions in the organisation's contract with the service provider or other third party should be more fulsome.

In addition, it is good practice for organisations to conduct due diligence on service providers and other third parties to whom they will transfer sensitive personal information, including: reviewing the third party's privacy policies and procedures; inquiring about safeguards the third party has implemented; inquiring about the third party's history of privacy complaints and data breaches; including audit rights in the applicable contract, and exercising such rights; and inquiring as to the location where the information will be stored, and considering the legal framework for privacy and data protection in the recipient jurisdiction(s) to determine risks to information stored in such jurisdiction(s).

5.4 Information provision and notification requirements

Under Section 13.1 of Alberta PIPA, if an organisation uses a service provider, including an affiliate that provides a service to the organisation, outside Canada to collect personal information about an individual on its behalf, or if the organisation directly or indirectly transfers personal information to a service provider outside Canada, the organisation must notify the individual at the time of collecting or transferring the information of the way in which they can obtain information about the organisation's policies and practices respecting foreign service providers, as well as the name or title of a person who can answer questions about the collection, use, disclosure or storage of personal information by the organisation's foreign service providers.

In addition, under Section 6(1) of Alberta PIPA, if the organisation uses a service provider outside Canada to collect, use, disclose or store personal information on its behalf, the organisation must develop and follow policies and practices that include: '(a) the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and (b) the purposes for which the service provider outside Canada has been authorised to collect, use or disclose personal information for or on behalf of the organisation.' The organisation must make written information about these policies and practices available on request.

There are no explicit statutory information requirements in any other jurisdiction. However, the OPC has indicated in past cases and guidelines that organisations should inform individuals that their information will be transferred outside Canada, and that it may be accessible to courts, law enforcement and national security authorities of the recipient jurisdiction(s). According to the OPC, providing such information is necessary to meet transparency and informed consent requirements, so that individuals understand the implications of providing their personal information to the organisation.

6. Sanctions & penalties

6.1 Criminal and civil liabilities

An individual affected by a breach of PIPEDA may, after receiving the OPC's decision, apply to the Federal Court for a hearing. The OPC can also apply to the Court for a hearing in respect of a complaint that it did not initiate, with the complainant's consent. The Court may: (1) order the organisation to correct its practices; (2) order the organisation to publish a notice of any action taken or proposed to be taken to correct its practices; and (3) award damages to the complainant, including damages for humiliation.

Under Section 60(1) of Alberta PIPA, if the Alberta Commissioner has made an order against an organisation for breach of the Act, the affected individual has a cause of action against the organisation for damages for loss or injury suffered as a result of the organisation's breach of the Act. In addition, if a person has been convicted of an offence under the Act, an affected individual has a cause of action against that person for damages for loss or injury suffered as a result of the conduct giving rise to the offence.

Under Section 57 of B.C. PIPA, if the B.C. Commissioner has made an order against an organisation for breach of the Act, or the organisation has been convicted of an offence, the affected individual has a cause of action against the organisation for damages for actual harm the individual suffered.

In addition, individuals can bring a civil claim for damages on the basis of the statutory and common law torts described in Section 1.1 above. However, the Court in *Jones v. Tsige*, 2012 ONCA 32 (CanLII) at para 70, indicated that non-pecuniary damages for the tort of intrusion upon seclusion are generally capped at CAN 20,000 (approx. €134,000).

6.2 Enforcement from regulatory authorities

Upon finding a breach of PIPEDA, the OPC can generally only make non-binding recommendations, except for certain offences, as follows:

'Every person who knowingly contravenes subsection 8(8), i.e., failing to retain information that is subject to an access request, or subsection 27.1(1), i.e., anti-reprisal provisions, or who obstructs the Commissioner or the Commissioner's delegate in the investigation of a

complaint or in conducting an audit is guilty of (a) an offence punishable on summary conviction and liable to a fine not exceeding CAN 10,000 (approx. €67,000); or (b) an indictable offence and liable to a fine not exceeding CAN 100,000 (approx. €670,000).'

Recent amendments to PIPEDA will also provide for similar potential fines if an organisation does not comply with the breach reporting and recording requirements of PIPEDA, once those requirements come into force.

Offences under Alberta PIPA are punishable by: '(a) in the case of an individual, to a fine of not more than CAN 10,000 (approx. €67,000); and (b) in the case of a person other than an individual, to a fine of not more than CAN 10,000 (approx. €67,000[6]).'

Offences under B.C. PIPA are punishable by: '(a) if an individual, to a fine of not more than $10,000, and (b) if a person other than an individual, to a fine of not more than CAN 100,000 (approx. €670,000[7]).' The organisation commits an offence if it[8]:

'(a) uses deception or coercion to collect personal information in contravention of this Act,

(b) disposes of personal information with an intent to evade a request for access to the personal information,

(c) obstructs the commissioner or an authorised delegate of the commissioner in the performance of [their] duties or powers under this Act,

(d) knowingly makes a false statement to the commissioner, or knowingly misleads or attempts to mislead the commissioner, in the course of the commissioner's performance of [their] duties or powers under this Act,

(e) contravenes section 54, i.e., anti-reprisal provisions, or

(f) fails to comply with an order made by the commissioner under this Act.'

Offences under the Quebec Act are punishable by fines ranging from CAN 1,000 (approx. €670) to CAN 100,000 (approx. €670,000) depending upon the nature of the offence, whether it is a first offence or a subsequent offence, and whether the offence is committed by an individual or an organisation (see ss. 91-93).

---

1. Every jurisdiction in Canada also has legislation governing protection of personal information by government bodies and institutions, which has some provisions applicable to the personal information of public sector employees. However, this Guidance Note focuses on private sector laws. The activities of public-sector employers are also subject to th under the Canadian Charter of Rights and FreedomsThe Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11. Accordingly, employees of public sector employers have a right to be secure against unreasonable search or seizure, which has been applied in the past to monitoring of employee computers – see *R. v. Cole*, [2012] 3 SCR 34, 2012 SCC 53 (CanLII).
2. *Jones v. Tsige*, 2012 ONCA 32 (CanLII), at 70.
3. *Jane Doe 464533 v ND*, 2016 ONSC 541, at 46.
4. See footnote 1., at s. 43.
5. See footnote 1, at ss. 44 and 45.
6. Section 59(2) Alberta PIPA.
7. Section 56(2) Alberta PIPA.
8. Section 56(1) Alberta PIPA.

© 2015 Cecile Park Publishing Ltd. All rights reserved