Sterling Backcheck

Legal Considerations for Background Screening in Canada

How to Develop Policies Specific to Your Organization's Needs

Background checks are subject to various rules set out in Canadian privacy, human rights and consumer reporting laws. To ensure they respect the rights of applicants and employees, organizations should be aware of their obligations and develop background checking policies that take into account their particular needs, risk tolerance and legal obligations.

We have put together a guide of the various federal and provincial laws in Canada which affect employment background checks. The content of this paper is strictly for informational purposes only and does not constitute legal advice. Since each organization has different hiring requirements, it is recommended to consult with legal counsel when creating and updating a background screening program.

Sterling Backcheck

Legal Framework

Privacy Laws

Privacy laws regulate the collection, use, disclosure and retention of personal information. Canada has many privacy laws. Each province and territory, as well as the federal jurisdiction, has a public-sector privacy law that applies to government agencies, crown corporations and other public-sector organizations.

At the federal level this is called the Privacy Act; at the provincial and territorial level various names are used, including the Freedom of Information and Protection of Privacy Act (FOIP or FIPPA) or the Access to Information and Protection of Privacy Act (ATIPPA).

For the private sector, there is a federal privacy law called the Personal Information Protection and Electronic Documents Act (PIPEDA), which regulates personal information collected by many organizations across Canada that are federally regulated or operate in provinces that do not have provincial privacy laws. Additionally, Quebec, B.C., Alberta and Manitoba[1] have enacted privacy laws that apply to organizations operating in those provinces.

Privacy laws differ in how and whether they apply to employees' and applicants' information. The guidelines on the following pages are general privacy concepts to keep in mind when developing a background check program.

Canada has many privacy laws. Each province, territory, and federal jurisdiction has a public-sector privacy law that applies to government agencies, crown corporations and other public-sector organizations.

[1] At the time of writing, Manitoba's Personal Information Protection and Identity Theft Prevention Act had not yet been proclaimed in force.

Notice and Consent

In most cases, privacy laws require that individuals be notified that their personal information will be collected and used, and the purposes for that collection. In addition, the individual often must consent to the collection and use of personal information. This may be true even in the case of publicly available information.

Limiting Collection, Use, Disclosure and Retention

When providing notice to an individual that personal information will be collected, the notice should include the purposes for the collection and how will the information be used? Then, only the personal information needed to achieve those purposes should be collected. Organizations should not collect extra details simply because they would be nice to have, or might be useful later. Each item of personal information must be justified.

Once the information has been collected, it can then only be used for the purposes you originally identified, unless the individual has agreed for it to be used otherwise. It cannot be repurposed for other uses. Disclosure is perhaps more intuitive; personal information is private, and should not be given out to other parties unnecessarily or without the consent of the individual or authorization under the law. Finally, personal information must not be retained forever. Retention periods should be established that satisfy business needs and legal obligations, and then personal information should be deleted once that time period is up.

Safeguards

Personal information under an organization's control must be carefully guarded against inadvertent loss or disclosure, using both physical and technological means. Organizations should carefully consider who should have access to background check information. Information revealed in a background check, even if the applicant is eventually hired, can be embarrassing for the individual. Access should therefore be strictly limited to a small group of trustworthy people.

Accuracy

Organizations have an obligation to ensure personal information in their custody is accurate, especially if it will be used to make a decision about an individual. This includes ensuring information is sourced properly. Many items should come from the individual directly to ensure accuracy, such as address history; other items must come from a third party to ensure accuracy, such as verification of prior employment.

Individual Participation

Individuals should be given access to their personal information on request, with a few exceptions as to what can (or must) be withheld. This allows them to dispute the accuracy of information. Disputes should be taken seriously and investigated to ensure personal information is accurate.

Accountability and Openness

Organizations should be prepared to answer questions about how—and why—they handle personal information. Individuals may ask for detailed information about why background check information is being collected and what exactly will be done with it. Having written policies in place can help reassure individuals that their privacy is taken seriously.

Non-compliance with privacy laws can result in time consuming investigations by privacy commissioners and reports that may name the offending organization and harm its corporate image and brand. It may also create a cause of civil action that could lead to expensive litigation and even monetary penalties. With the exception of Quebec, Canada's private-sector privacy laws do not currently allow regulators to fine companies that break the rules. However, legislative changes have been proposed that would beef up privacy commissioners' ability to aggressively enforce the law, so proactive compliance is certainly the best policy. In addition, even when a mistake is made, having good policies and procedures in place will help organizations more effectively respond to a privacy complaint or investigation.

Each item of personal information must be justified. Once collected, it cannot be repurposed for other uses unless the individual has given permission.

Sterling Backcheck

Human Rights Laws

Human rights laws exist in all jurisdictions in Canada. They are designed to prevent discrimination based on certain protected characteristics. Each jurisdiction (the ten provinces, three territories and the federal jurisdiction) has its own law with its own nuances, but many of the protected classes are similar. Some of the common protected classes include race, national or ethnic origin, sexual orientation, sex, gender identity, marital status, religion, age and disability. Some jurisdictions also protect criminal record information. Many other categories exist, and each jurisdiction defines these categories in different ways, so it is vital that organizations familiarize themselves with the laws that apply to them.

Generally speaking, federally regulated businesses like telecommunications and air transport are regulated by the Canadian Human Rights Act. For provincially regulated businesses, the applicable law may be the one that applies where the business is located, where the applicant resides, where the recruitment is happening or where the employment will take place. If these activities happen in more than one province or territory, multiple laws could apply.

Many categories of human rights laws exist in Canada. It is vital that organizations familiarize themselves with the laws that apply to them.

It is almost inevitable that organizations will come into contact with information identifying applicants' protected status during the recruitment, interview and background check process. Controls should be built into the process to mitigate this risk. **The following are a few examples of sensitive information that could appear on a background check:**

Social Media Searches

Many social media profiles, such as those on Facebook and Twitter, are primarily personal in nature. Applicants may mention age, religious or political affiliation, ethnic background or other information that you cannot use in an employment decision.

Drug and Alcohol Testing

Drug and alcohol testing may reveal information about an addiction, which may be considered a disability. This type of information can only be taken into account in very narrow circumstances where there is a bona fide job requirement.

Sterling Backcheck

Criminal Records and Police Information

Criminal records and police information require great care to avoid unfair discrimination. **This information is treated in different ways in different jurisdictions as shown in the table below:**

Jurisdiction (Law)	Pardoned Offences Protected	Unrelated Offences Protected	No Specific Protection
Alberta (Human Rights Act)			■
British Columbia (Human Rights Code)		■	
Federal (Canadian Human Rights Act)	■		
Manitoba (Human Rights Code)			■
New Brunswick (Human Rights Act)			■
Newfoundland and Labrador (Act Respecting Human Rights)		■	
Northwest Territories (Human Rights Act)	■		
Nova Scotia (Human Rights Act)			■
Nunavut (Human Rights Act)	■		
Ontario (Human Rights Code)	■		
Prince Edward Island (Human Rights Act)		■	
Quebec (Charter of Human Rights and Freedoms)	■	■	
Saskatchewan (Human Rights Code)			■
Yukon (Human Rights Act)		■	

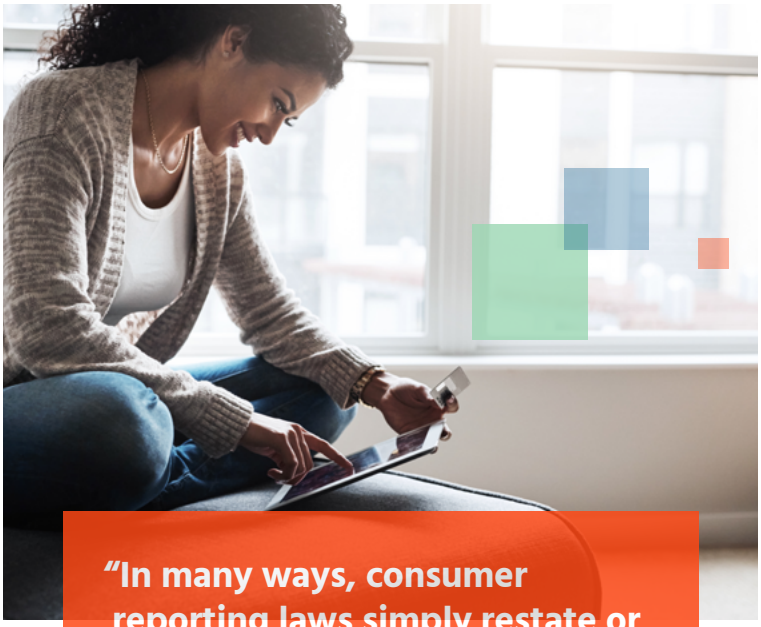
- Pardoned offences protected means that the law forbids discrimination based on criminal offences subject to a pardon or a record suspension.
- Unrelated offences protected means that the law restricts (but does not forbid) discrimination based on criminal history. In these jurisdictions, criminal history information can only be used if it is related to the position.
- No specific protection means that the law does not specifically protect criminal history. However, a human rights commission or tribunal could extend protections to information found in a criminal record check based on other provisions in the law.

Illegal discrimination or the appearance of it may result in a human rights complaint, which can lead to a time consuming and expensive investigation. Organizations found to have violated the law may be required to pay damages to the complainant, and in some cases, punitive damages can be awarded. Individuals can also file lawsuits over human rights violations. Having good practices and procedures in place to reduce the possibility of illegal discrimination may help respond to a human rights complaint or lawsuit.

Consumer Reporting Laws

Every province except New Brunswick has a law in place to regulate companies that create and deliver reports about individuals, including credit bureaus and background checking companies. These maybe specific laws about "consumer reporting," "credit reporting" or "personal investigations," or may fall under general consumer protection legislation. The territories do not have consumer reporting laws, and Quebec's consumer reporting law is the same as its private-sector privacy law—the Act respecting the protection of personal information in the private sector. In many ways, consumer reporting laws simply restate or strengthen some of the concepts in privacy law, like notice and consent, accuracy and the right to access personal information. Background checking companies are responsible for compliance with the majority of the provisions in consumer reporting laws, but the companies using the background checks also have some responsibilities, most notably:

- Notifying the applicant of the background check and obtaining consent in accordance with the technical requirements of the law;
- Notifying the applicant of an adverse decision based on information from the background check.



"In many ways, consumer reporting laws simply restate or strengthen some of the concepts in privacy law, like notice and consent, accuracy and the right to access personal information."

Conclusion

There are many laws, regulations and rules that govern the background screening industry. These laws aim to protect candidates when their personal information is used on an application and during background screening. To respect the rights of applicants and employees, organizations should be aware of their obligations and develop background checking policies that take into account their particular needs, risk tolerance and legal obligations.

The information provided in this background check compliance for Canada guide is intended for awareness and informational purposes only. It neither constitutes legal advice nor is a recommended approach. Organizations should design their programs in consultation with legal counsel. Organizations that operate outside of Canada should develop background check policies for those jurisdictions in accordance with local laws and best practices.

Sterling

About Us

Sterling Backcheck—Canada's industry leader in background and identity services—provides a foundation of trust and safety that spans across industries, professions and borders.

Our technology-powered services help organizations create great environments for their workers, partners and clients. Sterling Backcheck is part of Sterling, which has 20 offices in nine countries and conducts more than 100 million searches annually.

Want More?

In addition to this report, Sterling regularly publishes cutting-edge research and insight on the latest trends in human resources, talent management and hire processing.

For more information, visit us at: **sterlingbackcheck.ca**

sterlingbackcheck.ca | 866.881.2011