First Advantage Canada Privacy Policy

First Advantage Canada, Inc. ("FADV," "our", "us" or "we") provides background screening services for the purposes of and at the direction of its clients to assist them in considering individuals for employment, changes in the level of responsibility and other circumstances where an employee or prospective employee's background is relevant. This is achieved by preparing a background screening report for the client.

Please carefully read our privacy policy to understand how we will treat personal information provided to us by candidates ("you") and/or our client in the context of such background screening services. This policy may change from time to time. Please check the policy each time you use our site for the most current information.

Some of our subsidiaries and affiliates maintain their own privacy policies. Please refer to those unique websites directly for further information. This site is not intended for children and we do not knowingly collect any information about children.

How We Use and Collect Information in Our Specific Business Dealings

While international requirements vary, these acts all follow the same general principles: Privacy, Access, Accuracy, Fairness and Accountability.

As our main business operations for the performance of background screening services in Canada are in Canada, the following most specifically addresses our compliance requirements under the Personal Information Protection and Electronic Documents Act (PIPEDA).

We are committed to being an international leader in employee screening services by providing our clients the most accurate information and we take our role as a partner to our clients seriously. We believe in, and demonstrate, compliance and transparency in our business practices.

Summary of PIPEDA

PIPEDA applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity. Consent is required for the collection, use or disclosure of personal information about an individual. The individual has a right to access their personal information and to challenge its accuracy, if necessary. Personal information can only be used for the purposes for which it was collected and this purpose must be clearly noted to the individual. Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

Core Principles of PIPEDA

1. Accountability: An organization is responsible for the personal information under its control and shall designate an individual or individuals accountable for the organization's compliance with the following principles. This role is called a Privacy Officer.

2. Identifying Purposes: The purposes for which personal information is collected shall be clearly identified by the organization to the individual concerned, at or before the time the information is collected, and prior to any new use.

3. Consent: The knowledge and consent of the individual whose information is involved are required for the collection, use or disclosure of personal information, except where inappropriate.

4. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means only.

5. Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes.

6. Accuracy: Personal information shall be as accurate, complete and up-to-date as necessary for the purposes for which it is to be used.

7. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. This includes password-protected computers, shredding of documents and electronic retention of data as a preferred means to hard copy.

8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Personal Information

Personal information includes any information, recorded or not, about an identifiable individual. The types of personal information about candidates that FADV collects, uses and discloses are described below under the heading "What Personal Information does FADV Collect." Personal information does not include the name, title, business address or telephone number of an employee of an organization (e.g. the name, title, business address and/or business telephone number of a candidate's reference).

Consent

FADV requires the express written consent of individuals to deliver our services; this consent may be provided in hard copy or via electronic signature through our online platforms. In rare circumstances, FADV may be required to disclose personal information without the knowledge or consent of the

candidate. These include disclosure to a third party when required or authorized by law, regulation, search warrant, subpoena or court order; in situations involving the collection of a debt owned by the individual to the organization; in an emergency that threatens the life, health or security of an individual; or upon suspicion of an illegal activity.

A candidate may withdraw their consent by advising the applicable client who ordered the background check. We rely on our clients to explain to candidates the implications relevant to the client of the candidate withdrawing their consent. If in the course of our services, we are informed a candidate has withdrawn their consent, we will cease work on the file and confirm with the client this action.

Accountability

Ms. Rhonda Fairweather, General Manager, is our designated Privacy Officer and appointed representative for all privacy and records management issues. Ms. Fairweather has complete authority to investigate, enforce, educate, and ensure compliance with FADV's privacy policies and procedures. Clients and candidates may request a copy of or raise questions related to this privacy policy by contacting our Appointed Representatives at any time.

What Personal Information Does FADV Collect

Our company performs employment screening services for various companies and, depending on the nature of the client request, we may collect, use, disclose, transfer and retain some or all of the following personal information:

- Name / Maiden Name / Other Names (if applicable)
- Gender
- Date of Birth
- Social Insurance /Security Number
- Driver's licence number
- Current address / address history
- Passport number

This information is generally provided to FADV in written format on the following documents:

- Resume
- Client's official application form
- FADV's consent release form
- FADV's criminal consent release form

Additional information will only be collected if it is a requirement of completing the background check.

Identify the Purpose for Obtaining Personal Information

We receive personal information from our clients for the sole purpose of performing background checks on individuals. The personal information we require is dependent on the checks we need to complete and we ask our client and the candidate to only provide the personal information that is necessary. The

use of this information is strictly limited to the fulfilment of the client's request and will not be used by FADV for any other purpose.

NOTE: International searches may have unique and additional requirements. The candidate is made aware of the need for personal information:

- Verbally and in writing by the client
- By reading and signing the client's and FADV's consent form(s)

Once the information is in our possession, the candidate's personal information will be used specifically for this client's request and will not be used in association with any other request/search/client.

Obtain Consent

Depending on the services required by the client we will obtain consent through written forms only. When written consent is required to perform a service, FADV staff is required to retain a soft copy of this consent in the candidate's file.

Under PIPEDA, for consent to be valid, individuals must be able to understand the consequences of the collection, use or disclosure to which they are consenting. While FADV takes all reasonable measures to protect data, there is always inherent risk when providing personal information. We have procedures and practices to safeguard your personal information against loss, theft and unauthorized access.

Limiting Collection

FADV collects only the information about candidates that is listed above to perform the searches requested by clients and will only request additional information when it is needed for the successful completion of the check. If we do make this type of request our staff will document when and why we need the additional personal data. We will not use any of the candidate's personal information for any purpose other than to perform the checks as requested by the client.

We do not make any recommendations as to a candidate's suitability for employment and leave that decision solely to the discretion of the client.

If a client cancels a request we will not collect or pursue any outstanding information. We will submit a report to the client outlining all of the information we obtained and cancel all outstanding requests for information.

Once a file is archived only authorized administrative personnel and management are allowed to access this information. The date and reasons for accessing this information will be documented in the candidate's file.

Limit Use, Disclosure, and Retention

We will retain all documentation and personal data for each check we perform for a minimum period of two years. This will provide every candidate a reasonable amount of time in which to dispute any inaccuracies.

We will retain a soft copy of our findings (reports) for a minimum of two years (or whatever time period is required by our clients), after which this information is deleted from our databases.

We may share information you provide with affiliates, suppliers and/or sources in order to complete your background check. This includes the following:

- Suppliers and affiliates with whom we contract to complete background checks (we only provide these affiliates and suppliers the personal information necessary to run these checks);
- Past employers
- Educational institutions
- Professional licencing bodies
- Criminal/civil record sources
- Credit bureaus; and
- Online database holders

We will only send the results of the checks to the individual(s) who requested the checks or as directed by the administration of the account.

Accuracy

When our staff receives personal information which is unclear (i.e. difficult to read) we contact the client immediately and clarify the discrepancy. The client is then asked to provide clarification of same. We will not process any check without accurate information. The candidate also has the right to dispute the information we provide to the client if they believe it is inaccurate.

Use Appropriate Safeguards

Shredding of hard copies and deletion of electronic files is handled in a secure manner by FADV. All current and archived files containing personal data are housed in an office that is secured by lock and a security system. Files that are archived can only be accessed by authorized administrative personnel and management. We retain only soft copies of our final reports. Current soft copies are stored on the network, which is protected using a router -based firewall. A router is a safe and reliable means of protecting data because it provides two levels of security. Data is transmitted to and from our clients using fax, email, encrypted email, this online web interface and the telephone.

Be Open and Give Individuals Access to their Personal Information

Candidates can gain access to their personal information including their resume, list of references, and signed release forms, if applicable, by providing our Appointed Representative written notice. They must provide a legitimate reason for requesting the information and four personal identifiers, as requested, which may include date of birth, full name, social insurance number, and current and past addresses.

These will be used to verify the identity of the requestor before any information is released. Candidates who believe our company is in possession of inaccurate personal data that led to inaccurate checks or dispute the accuracy of our findings may write a letter which outlines the inaccuracy to our Appointed Representative. The candidate must also provide a copy of this letter to the client in question.

Our Appointed Representative will then have 30 days to investigate the issues and resolve any inaccuracies. Discrepancies, if any, will be communicated in writing to the client and candidate at the

same time. We will also make any corrections to our files at that time. If a candidate's request is, for any reason, denied they will receive a letter explaining why.

Challenging Compliance

If a candidate wishes to file a complaint and/or gain access to their personal information they may write to:

First Advantage Canada Inc.
C/O Rhonda Fairweather, Vice President, Operations
59 Adelaide Street East, Suite 300
Toronto, Ontario M5C 1K6

Candidates must clearly state the nature of their inquiry, the client name, and provide their mailing address and telephone number. They must also provide personal identifiers including date of birth, full name, social insurance number, and current and past addresses, which will be used to verify the identity of the requestor as well as a clear, legible copy of one piece of government-issued photo identification.

Access to personal information will be disclosed within 30 days. FADV will provide access to all personal information except that permitted under PIPEDA to be exempted from disclosure. We will acknowledge receipt of a complaint inquiry with a written letter that will be mailed or emailed to the address provided. This letter will reiterate the nature of the inquiry and provide the candidate with a tentative date when the issue will be resolved. We will record and file the initial inquiry as well as the letter to the candidate in our files. Once a decision has been rendered it will be mailed to the candidate. A copy will also be filed in our records. A copy of all documentation used to arrive at the decision will be copied and filed in our records.

If the candidate disputes the decision he/she has a right to contact the Privacy Commissioner of Canada at:

112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3