JARVIS

JARVIS CONSULTING GROUP
jrvs.ca

Privacy Policy

Personal Information Protection and Electronic Documents Act (PIPEDA)

Table of Contents

Introduction

Our Privacy Policy is effective as of February 15, 2024.

Last updates:

Update	June 24, 2024

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your personal information when You use the Service and tells You about Your privacy rights and how the law protects You.

This Privacy Policy is applicable to all natural persons that share personal information with Jarvis Consulting Group.

We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy.

This policy is based on the Personal Information Protection and Electronic Documents Act (PIPEDA) effective Jan 1, 2019.

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.
Definitions

For the purposes of this Privacy Policy:

- "Account" means a unique account created for You to access our Service or parts of our Service.

- "Client" refers to any natural or legal person who has entered into a contractual agreement with the Company to receive the Service.

- "Company" (referred to as either "the Company", “Jarvis Consulting Group”, "We", "Us" or "Our" in this Agreement) refers to Jarvis Consulting Group with their business seat at Suite 307 - 150 King Street West, Toronto, Ontario, M5H 3T9

- "Contractor" refers to any natural or legal person who, under contract, performs work or provides services to the Company outside of the context of an employment relationship.

- "Cookies" are small files that are placed on Your computer, mobile device or any other device by a website, containing the details of Your browsing history on that website among its many uses.

- "Country" refers to Canada.

- "Device" means any device that can access the Service such as a computer, a cell phone or a digital tablet.

- "Employee" refers to an individual who is in an employment relationship with the Company, or who has applied to the Company for employment.

- "Personal Data" is any information that relates to an identified or identifiable individual. Under PIPEDA, it refers to information about an identifiable individual, excluding business contact information. This could include but is not limited to, an individual’s name, residential address and telephone number, email address, social insurance number, physical description, and consumer preference information.

- “Privacy Officer” is an appointed individual within an organization accountable for ensuring compliance with privacy laws and regulations. This includes creating and implementing privacy policies and procedures, responding to privacy-related inquiries and complaints, educating staff on privacy obligations, ensuring the update of privacy practices as laws change, working closely with the legal team to mitigate potential privacy risks, and leading the response to any data breaches, including the necessary notifications and reporting.

- "Service" refers to the Website.

- "Service Provider" means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analyzing how the Service is used.

- "Usage Data" refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).

- "Website" refers to Jarvis Consulting Group web page, accessible from www.jrvs.ca

- "You" means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.

Collecting and Using Your Personal Data, Types of Data Collected and Personal Data

While using Our web-site, We may ask You to provide Us with certain personally identifiable information that can be used to contact or identify You. Personally identifiable information may include, but is not limited to:

●Email address
●First name and last name
●Phone number
●Address, State, Province, ZIP/Postal code, City
●Usage Data

Usage Data

Usage Data is collected automatically when using the web-site.

Usage Data may include information such as Your Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When You access web-site by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.

We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

Tracking Technologies and Cookies

We use Cookies and similar tracking technologies to track the activity on the web-site and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze Our Service. The technologies We use may include:

- Cookies or Browser Cookies. A cookie is a small file placed on Your Device. You can instruct Your browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if You do not accept Cookies, You may not be able to use some parts of our Service. Unless you have adjusted Your browser setting so that it will refuse Cookies, our Service may use Cookies.
- Web Beacons. Certain sections of our Service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on Your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close Your web browser.

We use both Session and Persistent Cookies for the purposes set out below:

- Necessary / Essential Cookies

Type: Session Cookies

Administered by: Us

Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.

- Cookies Policy / Notice Acceptance Cookies

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies identify if users have accepted the use of cookies on the Website.

- Functionality Cookies

Type: Persistent Cookies

Administered by: Us

Purpose: These Cookies allow us to remember choices You make when You use the Website, such as remembering your login details or language preference. The purpose of these Cookies is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

- Tracking and Performance Cookies

Type: Persistent Cookies

Administered by: Third-Parties

Purpose: These Cookies are used to track information about traffic to the Website and how users use the Website. The information gathered via these Cookies may directly or indirectly identify you as an individual visitor. This is because the information collected is typically linked to a pseudonymous identifier associated with the device you use to access the Website. We may also use these Cookies to test new pages, features or new functionality of the Website to see how our users react to them.

Use of Your Personal Data

For more information about the cookies we use and your choices regarding cookies, please visit our Cookies Policy or the Cookies section of our Privacy Policy.

The Company may use Personal Data for the following purposes:

● To provide and maintain our web-site, including to monitor the usage of our Service.
● To manage Your Account: to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.
● For the performance of a contract: the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.
● To contact You: To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.
● To provide You with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.
● To manage Your requests: To attend and manage Your requests to Us.
● For business transfers: We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.
● For other purposes: We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing and your experience.

We may share Your personal information in the following situations:

● With Service Providers: We may share Your personal information with Service Providers to monitor and analyze the use of our Service, to contact You.
● For business transfers: We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of Our business to another company.

We may collect your personal data from the following sources:

Directly from You (through forms, email, telephone, mobile phone, personally in conversation with You),

From other persons (e.g. from persons employed or otherwise engaged by your employer with whom we have entered into a service contract). In such cases, we rely on the fact that the persons that provide us with Your personal data or provide instructions for processing of the same have the sufficient authority to do so, and that they have provided you with all necessary

information regarding the processing of Your personal data, or have obtained your approval if necessary,

From publicly available sources (e.g. the Court Register, land registers and similar registers, sanctions lists and other publicly available information).
In the event that You have to provide to us personal data of other persons, it is your responsibility to ensure that the person whose personal data you provided has been informed about the same and accepts the manner in which we may use such personal data.

Retention of Your Personal Data collected on Web-site

The Company will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Transfer of Your Personal Data

Your information, including Personal Data, is processed at the Company's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to — and maintained on — computers located outside of Your state, province, country or other governmental jurisdiction where the data protection laws may differ from those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

Disclosure of Your Personal Data, Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

Law enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Other legal requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public
- Protect against legal liability

Security of Your Personal Data

The security of Your Personal Data is important to Us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, We cannot guarantee its absolute security.

Detailed Information on the Processing of Your Personal Data

The Service Providers We use may have access to Your Personal Data. These third-party vendors collect, store, use, process and transfer information about Your activity on Our Service in accordance with their Privacy Policies.
Analytics
We may use third-party Service providers to monitor and analyze the use of our Service.

Web-site Children's Privacy

Our Service does not address anyone under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data, please contact Us. If We become aware that We have collected Personal Data from anyone under the age of 13 without verification of parental consent, We take steps to remove that information from Our servers.

If We need to rely on consent as a legal basis for processing Your information and Your country requires consent from a parent, We may require Your parent's consent before We collect and use that information.

Links to Other Websites

Our Service may contain links to other websites that are not operated by Us. If You click on a third party link, You will be directed to that third party's site. We strongly advise You to review the Privacy Policy of every site You visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Consent Form and Agreement

By visiting our web-site, You are consenting to the collection and use of your Personal Data as outlined in this Privacy Policy. We may require You to provide consent to the updated Privacy Policy in a specified manner before further use of the Service is permitted. If you do not agree, you should discontinue use of the Service.

In some cases, we may provide you with a form to specifically acknowledge your understanding of certain aspects of our Privacy Policy. The form may include, but is not limited to the following:

- Full Name
- Email Address
- Contact Details (Phone Number, Home Address)
- Usage data and browsing history on the Company's website

By filling out this form, you are providing explicit consent for the collection, use and disclosure of your Personal Data as outlined in the form and this Privacy Policy.

Withdrawal of Consent

You have the right to withdraw your consent to the processing of your Personal Data at any time. If you would like to withdraw your consent or change your preferences, you may do so by contacting admin@jrvs.ca. Please note that this will not affect the lawfulness of the processing before the withdrawal.

Third Parties

We will not share your information with any third parties or affiliates including ones who provide services to us and to support the delivery of, provide functionality on, or help to enhance the security of our Website.

10 DLC Compliance Statement

As part of our dedication to regulatory compliance and transparent communication practices, we operate in accordance with the 10 Digit Long Code (10 DLC) program for text messaging. By utilizing our messaging services, you agree to receive communications that adhere to 10 DLC guidelines. Your phone number and messaging interactions are handled securely and are not disclosed to external parties. You may opt out of receiving messages at any time by replying "STOP" to our messages.

Right to Represent

When recruiting, we may ask for your consent to process your Personal Data. This is often referred to as the "Right to Represent". This is a specific permission granted by you, allowing us to process your Personal Data for a particular purpose.

For example, we may need your consent to use your Personal Data to submit your application for a specific job opportunity, or to share your details with a potential employer. In these situations, we will provide you with full details of the information we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us. Moreover, once given, you have the right to withdraw your consent at any time.

Onboarding process and personal info we collect from You

During the onboarding process, we collect personal data from you under your specific or implied consent. The type of information we collect includes:

- Address
- Emails
- Cell Phone Numbers, contractors and candidates in a recruitment and onboarding process such as:

J

- Legal name and surname
- Social Insurance Number
- ID proof (Identification Card, Driving Licence or Passport)
- Canadian Citizenship Card
- Possession and Acquisition Licence or PAL Card
- Permanent Residency Card
- Certificate of Indian Status
- Canadian National Institute of Blind (CNIB) Identification Card
- Canadian Military Employment Card or Canadian Military Family Identification Card
- International Student Card
- Birth Certificate
- Bapstismal Certificate
- Hunting License
- Outdoors card
- Canadian Blood Donor Card
- Immigration Papers
- Education certificate
- Home address
- email address
- Cell Phone Number

Offboarding process and destruction of your personal information.

When your relationship with our company ends, whether through termination of contract, completion of engagement, or other circumstances, we implement an offboarding process to ensure the secure handling and destruction of your personal data.

- Retention Period: We retain your personal data only as long as necessary to fulfill the purposes for which it was collected. This includes satisfying any legal, accounting, or reporting requirements.

- Data Deletion: Once the purpose for holding your personal data has been fulfilled, and after any mandated retention period has expired, your personal data will be deleted or destroyed in a secure manner. This includes digital data and any physical copies of personal data.

- Data Destruction: The destruction of data will be undertaken in a manner that ensures the information cannot be reconstructed or retrieved. Digital data will be permanently erased from all systems and physical data will be shredded or otherwise irretrievably destroyed.

- Record Keeping: For auditing purposes, we maintain a record of the personal data that has been deleted or destroyed. This record will include the type of data, the date of destruction, and the reason for destruction.

- Notification: Whenever possible and applicable, we will inform You about the deletion or destruction of your personal data.

Storage of Personal Information of Jarvis Employees, Contractors and Clients

We store all collected personal information on trusted systems such as BullHorn, IntelliHR, and Google Drive. These platforms are renowned for their robust security measures and are trusted by businesses worldwide for data storage.

To ensure the safety of your personal information, we implement various security measures. These include physical security measures and electronic safeguards to prevent unauthorized access, alteration, disclosure, or destruction of your data.

Access to the stored personal information is limited to authorized Jarvis Technologies Group Inc. personnel only. These individuals are bound by strict confidentiality agreements, requiring them to use the information in compliance with our privacy policy.

We strive to maintain the accuracy, completeness, and up-to-dateness of the personal information we hold. Employees, contractors, and clients can request to access, correct, or delete their personal information at any time.

Retention and transfer of Personal Information

We do not store, transfer, or make available ("Store" or "Storage") Personal Information outside of the regions with robust data protection laws and regulations, ensuring the safeguarding of personal information. These regions include:

- Canada and The United States, where we adhere to their respective privacy laws and regulations for storing and transferring personal data.

- The Member States of the European Union and The European Economic Area, where we comply with their stringent data protection laws for handling personal data.

- Any countries or states that have been subject to an adequacy decision as per Article 45 of the European General Data Protection Regulation (EU/2016/679). Here, we only store, transfer, or make available personal information in those regions recognized by the EU as having an adequate level of data protection.

These regions, collectively referred to as "Adequate Countries", allow us to ensure the continued protection of personal data in line with our stringent privacy standards and regulatory obligations. We will not store personal data in any location not recognized as an Adequate Country without the explicit consent of the data subject.

Access and Correction

You have the right to request access to the Personal Data we hold about You in order to verify the Personal Data we have collected in respect to You and to have a general account of our uses of that information. Upon receipt of your written request, we will provide you with a copy of your Personal Data, although in certain limited circumstances, and as permitted under law, we may not be able to make all relevant information available to you, such as where that information also pertains to another user. In such circumstances we will provide reasons for the denial to You upon request. We will endeavor to deal with all requests for access and modifications in a timely manner.

Audits and Inspections

We conduct regular audits and inspections of our data handling practices and policies, with a full audit taking place every 12 months.These audits are rigorous and comprehensive, covering all aspects of our data storage, transfer, and access protocols. They serve as an essential tool for ensuring our ongoing compliance with privacy laws and regulations, as well as identifying any areas for improvement.

In addition to our internal audits, we also welcome external auditors to review our data and policies. This external perspective provides an additional layer of scrutiny, ensuring that our practices meet or exceed industry standards and regulatory requirements.

Furthermore, we understand the importance of traceability in ensuring the integrity of our data. For this reason, we have implemented robust tracking systems that record all changes made to

our data. This allows us to provide credible proof of our actions and maintain a comprehensive record of changes.

Trainings and Onboarding procedure

We have implemented a comprehensive privacy training policy for all our employees and contractors.

Before commencing employment with us, all new hires, whether employees or contractors, are required to read and understand our Privacy Policy. This crucial first step ensures that they are aware of our commitment to personal data protection and understand the responsibilities that come with handling personal information.

In addition to this initial introduction, privacy training is also an integral part of our onboarding process. All Employees and Contractors receive comprehensive training on our Privacy Policy and related procedures as soon as they join the company. This training is designed to provide a thorough understanding of our data protection principles, the importance of privacy, and their role in maintaining these standards.

Moreover, this training is not a one-time process. We believe in the importance of continuous learning to keep pace with the evolving data protection landscape. Therefore, we provide regular updates and refresher courses to ensure that all team members stay informed about any changes to our Privacy Policy or relevant data protection laws and regulations.

Personal Data Breach Incident Response

Our company values and respects the privacy and security of personal data. In the event of a personal data breach, we have an established Incident Response Plan to manage such situations.

- Identification and Validation: Upon discovery of a potential breach, our team, led by our designated Privacy Officer, will verify and assess the nature and extent of the incident. Our Privacy Officer has been specifically trained to handle such incidents and will ensure that all necessary steps are taken swiftly to identify, contain, and address the breach..

- Containment and Eradication: Once a breach has been confirmed, we will take immediate action to contain and eliminate the threat.

- Investigation: We will conduct a thorough investigation to understand the cause and impact of the breach.

- Notification: If a breach involves the personal data of our clients, we will notify them as soon as possible and provide information about the nature of the breach, the type of data involved, and any measures taken to mitigate the situation. The specifics of such notification can be defined in individual client agreements.

- Recovery: We will implement measures to recover lost data, if possible, and restore any compromised systems to normal operations.

- Reporting: We will document the incident, its impact, and our response, maintaining this information for our records and for any necessary legal or regulatory reporting.

- Review and Update Procedures: After the incident, we will review our practices and procedures, identifying and implementing any necessary improvements to prevent future breaches.

Updates to this Privacy Policy

We may update our Privacy Policy from time to time. Any changes we make to our Privacy Policy in the future will be posted on this page and, where appropriate, notified to you by email. Please check back frequently to see any updates or changes to our Privacy Policy.

Contact Us

If You have any questions about this Privacy Policy, You can contact us:

●By visiting this page on our website: www.jrvs.ca
●By sending an email to Privacy Officer: admin@jrvs.ca

In the event that You are not satisfied with our response, You can submit a complaint to The Office of the Privacy Commissioner of Canada (OPC), 30 Victoria Street, Gatineau, Quebec K1A 1H3, e-mail: info@priv.gc.ca, website: https://www.priv.gc.ca/en/report-a-concern/