

SHERPA° – PRIVACY POLICY

INTRODUCTION

Welcome to sherpa's Privacy Policy (the **Policy**).

This version of the Policy was last updated on **August 3, 2022**.

Sherpa° respects your privacy and is committed to protecting your personal data. This Policy will inform you as to how we look after your personal data when you visit our websites or use any of our services (regardless of where you visit our websites from or where you access and use our services) and tell you about your privacy rights and how the law protects you.

This Policy is provided in a layered format so you can navigate to the specific areas set out below. The [Glossary](#) has been provided to help you understand the meaning of some of the terms used which are not defined in the body of this Policy.

CONTENTS

1	IMPORTANT INFORMATION; WHO WE ARE; OUR SERVICES	2
2	HOW IS YOUR PERSONAL DATA COLLECTED?	5
3	HOW WE COLLECT AND USE YOUR PERSONAL DATA	6
4	DATA SHARING	8
5	TRANSFERS TO GOVERNMENT ORGANIZATIONS	8
6	DATA SECURITY	9
7	DATA RETENTION	9
8	YOUR LEGAL RIGHTS	9
9	IF YOU ARE LOCATED IN THE UNITED KINGDOM OR EUROPE	11
10	IF YOU ARE LOCATED IN CANADA	14
11	GLOSSARY	15
12	HOW TO CONTACT US	16

1 IMPORTANT INFORMATION; WHO WE ARE; OUR SERVICES

PURPOSE OF THIS POLICY

This Policy aims to give you information on how sherpa° collects and processes your personal data through your use of our website, including any data you provide through our websites when you purchase or use any services that we provide. For the purposes of this Policy, references to our “websites” also includes our plug-ins and applications which are used or accessed on third-party websites to receive our services.

It is important that you read this Policy together with any other privacy policy we provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This Policy supplements other notices and privacy policies and is not intended to override them.

YOU MUST BE A LEGAL ADULT TO PURCHASE OUR SERVICES

Our websites and our services are not intended for use by children or those under the legal age of consent in the location where you access the websites or use any of our services (each, a **Minor**). We will only knowingly collect data relating to Minors if that data is provided to us by a legal adult making a purchase, and only if that data is required for us to facilitate an application for a visa or travel authorization in the name of that Minor submitted by you.

You must only provide us with personal data about any individual other than yourself if you have obtained permission from that individual to provide us with that information (and in the case of a Minor, are the parent, legal guardian, or authorized representative of that Minor).

WHO IS RESPONSIBLE FOR THIS PRIVACY POLICY

VISA RUN INC. (operating as **sherpa°**), an Ontario corporation with a business address at 340 King Street East, Toronto, Ontario, Canada M5A 1K8, is the controller under applicable privacy laws and is responsible for your personal data (referred to as “sherpa°”, “we”, “us” or “our” in this Policy).

We have appointed an authorized representative who is responsible for addressing questions in relation to this Policy. If you have any questions about this Policy, including any requests to exercise your legal rights, please [contact](#) us using the details set out below.

CHANGES TO THE PRIVACY POLICY AND YOUR DUTY TO INFORM US OF CHANGES

We keep our Policy under regular review. If we make changes to this Policy, those changes will not take effect until an updated version of this Policy is published on our websites. This version was last updated on the date noted at the beginning of this Policy. It is important that you review and understand the terms of the most current version of this Policy whenever you visit our websites or purchase any of our services.

It is important that the personal data we hold about you is accurate and current. To the extent that we have retained any personal data in a manner which can be used to identify you in accordance with this Policy, please keep us informed if your personal data changes during your relationship with us.

THIRD-PARTY LINKS

From time to time our websites will include links to third-party websites, plug-ins, and applications, and our services will be provided on third-party websites, or be made available to you on those websites through plug-ins and applications. Selecting those links, enabling those connections, or using our service through a third-party website or a plug-in or application on that website, may allow third parties to collect or share data about you and that data may include your personal data. We do not control those third-party websites and are not responsible for their privacy statements. When you leave our websites or use our services through a third-party website, we encourage you to read the applicable privacy policy of each of those relevant websites as the third parties are the controllers and are responsible for the processing of your data under those policies.

THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We collect, use, store and transfer different kinds of personal data about you in relation to visiting our websites or using our services which we have grouped together as follows:

- **Identity Data** including names, title, and usernames or similar identifiers, for example your passport information.
- **Contact Data** including address, email address, and telephone numbers.
- **Financial Data** including bank account and/or payment card details (redacted, to the extent it is provided to us by our payment processor for the purpose of managing your order for services).
- **Technical Data** including internet protocol (IP) address, your login data (if relevant), browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access our websites.
- **Profile Data** including your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- **Usage Data** including information about how you use our websites.
- **Transaction Data** including details about payments to and from you and other details of services you have purchased from us.

To the extent required in relation to your use of certain services that we provide to facilitate your visa or travel authorization applications (and/or as required by Government Organizations in relation to those applications), you will need to provide us with Transaction Data which contains certain personal data, including:

- Full name
- Aliases
- Date of birth
- Place of birth
- Nationality
- National identification number (excluding U.S. Social Security Numbers)

- Additional nationalities/citizenships
- Global Entry numbers
- Parent details (full name, place of birth, country of birth, nationality)
- Home address
- Telephone number
- Email address
- Employment status
- Occupation
- Education level
- Marital status
- Spouse details (full name, place of birth, country of birth, nationality)
- Employer details (name, address)
- Passport details (name, number, issue date, expiry date, issuing authority, type)
- Any existing or previously issued or rejected visas/travel authorizations
- Emergency contact (name, telephone number, email address)
- Trip details (purpose of travel, arrival date, port of arrival, places to be visited, first address of stay)
- Service confirmation numbers
- Payment information (credit/debit card numbers, card type, name on card, expiration dates, issuing bank, billing address, security code)
- Any other personal data which is required by a Government Organization from time to time in relation to applications for visas and/or other applicable travel authorizations

To the extent required in relation to your use of certain services that we provide to facilitate your visa or travel authorization applications (and/or as required by Government Organizations in relation to those applications), you will need to provide us with us with Transaction Data which contains certain **Special and Sensitive Categories of Personal Data**, including:

- Gender/sex
- Visible identifying marks
- Religion
- Ancestry
- Criminal record existence
- Health issue existence
- Legal questions, by way of example:
 - Have you ever violated any law related to possessing, using, or distributing illegal drugs?

- Have you ever been denied a visa you applied for with your current or previous passport, or have you ever been refused admission to a particular country or withdrawn your application for admission at any country's port of entry?
- Have you travelled to, or been present in particular countries on or after certain specific dates?
- Photographs (passport-type headshot photograph; photograph/scan of passport or other official form of identification, including of payment cards [to the extent payment cards are permitted as identification by an applicable Government Organization, or if used by a Sub-Processor for the purpose of processing payment for services])
- Any other Special Categories of Personal Data which are required by a Government Organization from time to time in relation to applications for visas and/or other applicable travel authorizations

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will **not** directly or indirectly reveal your identity. For example, we aggregate your Usage Data to calculate the percentage of users accessing a specific website or service feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Policy.

To the extent you are required to make a payment to us before using any of our services, we will use an independent third-party payment processor that complies with current Payment Card Industry Security Standards (PCI DSS) to accept and manage your Cardholder Data and facilitate your payment. We will never receive your full Cardholder Data, although we will receive limited information about your transaction and/or the payment method used (including some redacted Cardholder Data and/or a payment confirmation reference number) from the third-party payment processor for the purposes of allowing us to process and deliver the services that you requested.

IF YOU FAIL TO PROVIDE PERSONAL DATA

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we will not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with services). In that case, we will cancel an order you have placed for a service with us but we will notify you if this is the case at the time.

2 HOW IS YOUR PERSONAL DATA COLLECTED?

We use different methods to collect data from and about you from time to time including through:

- **Direct interactions.** You give us your personal data by filling in forms or by corresponding with us by telephone, email, submitting a form online, or otherwise. This includes personal data you provide when you:
 - apply for our products or services;
 - create an account on our website;
 - subscribe to our services or publications; or
 - give us feedback or contact us.

- **Automated technologies or interactions.** As you interact with our websites or use our services, we automatically collect Technical Data about your equipment, browsing actions, and usage patterns. We collect this personal data by using cookies, server logs, pixel tags, and other similar technologies. We also receive Technical Data about you if you visit other websites employing our cookies. Please see our Cookies Policy for further details. We may use automated tools or techniques, where those features are made available to you, to collect your personal data using optical scanning technology.
- **Third parties or publicly available sources.** We receive personal data about you from various third parties and public sources to the extent relevant to your use of our websites or services as set out below:
 - Technical Data from the following parties:
 - (a) analytics providers such as Google and Amplitude;
 - (b) providers of technical, payment and delivery services such as Stripe;
 - (c) providers of optical scanning technology such as Regula Forensic Science Systems; and
 - (d) publicly available sources.

3 HOW WE COLLECT AND USE YOUR PERSONAL DATA

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you to help facilitate your visa or travel authorization application.
- To carry out our obligations and enforce our rights arising from any contracts with you, including for billing and collection.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data, however:

- In relation to your use of our websites, we will get your consent before sending you third-party communications such as marketing to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.
- In relation to providing you with any of our services, including without limitation in facilitating your visa or travel authorization applications: (i) we will confirm that you have read and understand this Policy and consent to us providing your personal data to the applicable Government Organizations; (including in relation to Special Categories of Personal Data, where applicable) and (ii) our third-party payment processor will ask you to consent to their terms and conditions and privacy policy prior to accepting your payment information. You have the right to withdraw that consent at any time, provided that if you do so we will not be able to provide you with our services, and our payment processor will not be able to accept your payment.

COOKIES

You can set your browser to refuse all or some browser cookies or to alert you when websites set or access cookies. If you disable or refuse cookies on our websites or on any third-party website where you use our services, please note that some parts of our websites and/or our services are likely to become inaccessible or not function properly. For more information about the cookies we use, please see our Cookies Policy.

CHANGE OF PURPOSE

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please [contact us](#).

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we will process your personal data without your knowledge or consent, in compliance with this Policy, where this is required or permitted by law.

4 DATA SHARING

We will share your personal data with the external parties set out below to the extent necessary for the purposes set out in this Policy.

- Service providers who provide payment processing and IT and system administration services, including:
 - Google Cloud, based in the United States of America;
 - Stripe, based in the United States of America;
 - Zendesk, based in the United States of America;
 - SendGrid, based in the United States of America;
 - Zapier, based in the United States of America;
 - Unbabel, based in the United States of America; and
 - Terraform, based in the United States of America.
- Canada Revenue Agency and other authorities based in various jurisdictions who require reporting of processing activities in certain circumstances.
- Government Authorities based in various countries who require your personal data in relation to considering your application for a visa or travel authorization.
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners will use your personal data in the same way as set out in this Policy.
- Professional advisors, regulators, and auditors.

To the extent we are able to do so, we require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

5 TRANSFERS TO GOVERNMENT ORGANIZATIONS

Due to the nature of the services we provide, we will be required from time to time to transfer your personal data outside of the country where it is received by us to certain Government Organizations for the purpose of facilitating your visa or travel authorization applications. We will ask for your consent before we provide your personal data to those Government Organizations. In using our services, please be aware that:

- Those Government Organizations are independent from us.
- Each Government Organization is receiving and using your personal data because you requested and gave us permission to send that data to the Government Organization.
- We have no responsibility for or ability to control any Government Organization, including without limitation in relation to how those Government Organizations secure, use, process, and transmit your personal data.

Further information about the privacy policies and safeguards associated with each Government Organization can be found on their respective websites, or by contacting the relevant Government Organization directly.

6 DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal data, we cannot guarantee the security of your personal data transmitted to our websites or as a result of your use of our services. Any transmission of personal data is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on our websites or any part of our services.

For further information about the security measures we use, please [contact us](#).

7 DATA RETENTION

HOW LONG WILL YOU USE MY PERSONAL DATA?

We will only retain your personal data for as long as reasonably necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We will retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

In some circumstances you can ask us to delete your data—[see below for further information about your legal rights](#).

In some circumstances we will anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we will use this information indefinitely without further notice to you.

8 YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data which we have in our possession (if it has not been aggregated and anonymized). You have the right to:

- **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you at the time we receive your request and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, although we will need to verify the accuracy of the new data you provide to us.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we will not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we will demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- **Request restriction** of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
 - if you want us to establish the data’s accuracy;

- where our use of the data is unlawful but you do not want us to erase it;
 - where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **Request the transfer** of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data that we have in our possession at the time we receive your request in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
 - **Withdraw consent** at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we will not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please [contact us](#).

NO FEE USUALLY REQUIRED

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we can elect to charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive, or otherwise as permitted by applicable data protection laws. Alternatively, we could refuse to comply with your request in these circumstances.

WHAT WE NEED FROM YOU

We will from time to time need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We can also contact you to ask you for further information in relation to your request to speed up our response.

TIME LIMIT TO RESPOND

We will respond to requests in accordance with applicable data protection law. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

9 IF YOU ARE LOCATED IN THE UNITED KINGDOM OR EUROPE

The provisions in this section are supplemental terms which apply in addition to the remainder of this Policy if you are located in the United Kingdom or Europe.

We will comply with applicable data protection law. This says that the personal data we hold about you must be:

- used lawfully, fairly, and in a transparent way;

- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and to the extent appropriate, kept up to date;
- kept only as long as necessary for the purposes we have told you about; and
- kept securely.

For the purposes of applicable data protection law, sherpa° is the controller of your personal information. This means that we are responsible for deciding how we hold and use personal information about you. We are required under applicable data protection law to notify you of the information contained in this Policy.

We have appointed an authorized representative who is responsible for addressing questions in relation to this Policy. If you have any questions about this Policy, including any requests to exercise your legal rights, please [contact](#) us using the details set out below.

You have the right to make a complaint at any time to the relevant data protection authority, as set out below:

- The relevant data protection authority in the United Kingdom is the [Information Commissioner's Office \(ICO\)](#), and you can contact the ICO by calling +44 303 123 1113 or using its [live chat service](#).
- [See more information about the relevant data protection authority for other countries in the European Union](#) and how to contact those authorities.

We would, however, appreciate the chance to deal with your concerns before you approach the data protection authority, so please contact us in the first instance.

PURPOSES FOR WHICH WE WILL USE YOUR PERSONAL DATA

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we can process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please [contact us](#) if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you (to provide you with the requested service)

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To facilitate your application for a visa or travel authorization, including without limitation providing your personal data to the relevant Government Organization	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Technical	(a) Performance of a contract with you (to provide you with the requested service) (b) Necessary for our legitimate interests (to ensure that we have the appropriate information needed to provide you with the requested service)
To provide our services, including to process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Technical (f) Profile (g) Usage	(a) Performance of a contract with you (to provide you with the requested service) (b) Necessary for our legitimate interests (to receive payment for our services and recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or Policy (b) Asking you to leave a review, take a survey, or provide feedback	(a) Identity (b) Contact (c) Profile	(a) Performance of a contract with you (to provide you with the requested service) (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To administer and protect our business and our websites (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganization exercise)

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
	(d) Profile	(b) Necessary to comply with a legal obligation
To use data analytics to improve our websites, products/services, customer relationships, and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our websites updated and relevant, to develop our business and to inform our business strategy)
To make suggestions and recommendations to you about goods or services that are likely to be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)

TRANSFERS OUT OF THE UNITED KINGDOM AND EUROPE

Whenever we transfer your personal data out of the European Economic Area (EEA) or United Kingdom we use various methods to protect that personal data by implementing at least one of the following safeguards:

- We will transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission or the UK government, as applicable. For further details, see [European Commission: Adequacy of the protection of personal data in non-EU countries](#) and [Receiving personal data from the EU/EEA and third countries which have EU adequacy decisions](#).
- Where we use certain service providers, we use specific contracts approved by the European Commission or the UK government as applicable, which give personal data the same protection it has in the EEA and the United Kingdom. For further details, see [European Commission: Model contracts for the transfer of personal data to third countries](#) and [UK International data transfer agreement and guidance](#).
- Where we use third-party service providers based in the US, we may transfer data to them if they are part of any future scheme (such as the Trans Atlantic Data Privacy Framework) which requires them to provide similar protection to personal information shared between Europe and the US, as and when this is approved by the US and the EU. For further details, see [European Commission: EU-US Data Transfers](#).

Where these options are not available in relation to a particular Government Organization and/or country, and a transfer of your personal data to that Government Organization or country is required as a part of the services you requested from us, we will send your personal data to that Government Organization or country at your request and for the purpose of performing our contractual obligations to you. We will not send your personal data to that Government Organization or country unless you have provided us with your consent to do so.

Please [contact us](#) if you want further information on the specific mechanism used by us when transferring your personal data out of the UK and EEA.

10 IF YOU ARE LOCATED IN CANADA

The provisions in this section are supplemental terms which apply in addition to the remainder of this Policy if you are located in Canada.

We will only use your personal information in accordance with this Policy unless otherwise required by applicable law. We take steps to ensure that the personal information that we collect about you is adequate, relevant, not excessive, and used for limited purposes.

Privacy laws in Canada generally define “personal information” as any information about an identifiable individual, which includes information that can be used on its own or with other information to identify, contact, or locate a single person. For the purposes of this Policy, the terms “personal information” and “personal data” are used interchangeably.

DISCLOSURE OF YOUR INFORMATION

We may disclose personal information that we collect or you provide [as described in this Policy](#). We may also disclose your personal information:

- To comply with any court order, law, or legal process, including to respond to any government or regulatory request, in accordance with applicable law.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of our company, our customers, or others. This may include exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

TRANSFERRING YOUR PERSONAL INFORMATION

- We may transfer personal information that we collect or that you provide as described in this Policy.
- We may process, store, and transfer your personal information in and to a foreign country, with different privacy laws that may or may not be as comprehensive as Canadian law. In these circumstances, the governments, courts, law enforcement, or regulatory agencies of that country may be able to obtain access to your personal information through the laws of the foreign country.
- You are welcome to [contact us](#) to obtain further information about our policies regarding service providers that we may use outside of Canada.

- By submitting your personal information or engaging with our websites, you consent to this transfer, storage, or processing.

ACCESSING AND CORRECTING YOUR PERSONAL INFORMATION

By law you have the right to request access to and to correct the personal information that we have in our possession, provided that:

- We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.
- We will provide access to that personal information, subject to exceptions set out in applicable privacy legislation.
- We may charge you a fee to access your personal information, however, we will notify you of any fee in advance.
- Applicable law may allow or require us to refuse to provide you with access to some or all of the personal information that we hold about you.
- If we cannot provide you with access to your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

If you are concerned about our response or would like to correct the information provided, you may [contact us](#) for assistance.

CONTACT INFORMATION

To discuss our compliance with this policy, or if you have any questions, comments, or requests regarding this policy and our privacy practices, please [contact us](#).

11 GLOSSARY

Cardholder Data is a subset of personal data and means bank account or credit/debit card account numbers that identifies the issuer and the particular cardholder account plus any of the following: Account and sorting/routing numbers, cardholder name, expiration date and/or service code and sensitive authentication data including security-related information used to authenticate cardholders and/or authorize payment card transactions. The definition of Cardholder Data shall be consistent with the definition of Cardholder Data defined by the current Payment Card Industry Data Security Standards (PCI DSS).

Lawful Basis

- **Legitimate interest** means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we

process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

- **Performance of a contract** means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.
- **Comply with a legal obligation** means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

Government Organization means the third-party consultants, government organizations, or their authorized agents which your personal data is submitted to for the purpose of facilitating your application for a visa or travel authorization application through our services.

You collectively refers to all of the following individuals in relation to whom we process personal data:

- any natural person who visits our websites for any reason;
- any natural person who uses any of our services;
- any natural person who is providing us with any data of another individual with that individual's permission for the purposes of allowing us to facilitate an application for a visa or travel authorization in the name of that individual; and
- any natural person providing us with any data of a Minor who is a parent, legal guardian, or lawfully authorized representative of that Minor for the purposes of allowing us to facilitate an application for a visa or travel authorization in the name of that Minor.

12 HOW TO CONTACT US

If you have any questions or comments about this Policy or our privacy practices, please email us at privacy@joinsherpa.com.

[End of document]