

PRIVACY POLICY

1. INTRODUCTION

At Ventura Payments Ltd (hereinafter also – **Ventura Payments, Company** or **we**), we highly value your privacy and are dedicated to upholding the confidentiality and security of your personal information.

The purpose of this Privacy Policy is to offer you transparent and comprehensible insights into how we collect, utilize, and safeguard your data in accordance with Canadian data protection laws, including the Personal Information Protection and Electronic Documents Act (PIPEDA), and the General Data Protection Regulation (GDPR).

You are kindly requested to carefully review this Privacy Policy to gain a thorough understanding of our practices and their implications for you.

By opting to use our services, you indicate your acceptance of the terms outlined in this Privacy Policy.

We have exercised all reasonable efforts to ensure that these terms are clear, concise, and easily understandable. However, should you still have any questions or concerns regarding any aspect of our privacy practices, please feel free to reach out to us using the following contact details:

Ventura Payments Ltd

Address: 101-3704 32 STREET, VERNON, BRITISH COLUMBIA, V1T 5N6, Canada

E-mail: support@venturapayments.com

2. TYPES AND SOURCES OF INFORMATION

2.1. Sources

We may collect personal data from several sources to fulfill the objectives outlined in this Privacy Policy. These sources may include the following:

- Direct Sources – in cases when:
 - Information is provided directly by you (for example, when you create an account with us or use our services; when you make transactions using our platform; when you communicate with us or provide feedback on our services, etc.).
 - Information is gathered by automated technologies (for example, when information is automatically gathered through technologies like cookies and log files as you engage with our website and services).
- Indirect Sources – in cases when we gather information from third parties (for example, when information is received from payment processors, identity verification, publicly accessible sources and similar).

2.2. Types of information

For the purposes outlined in this Privacy Policy, we may process data primarily falling under the following categories:

- Personal Identity Related Data: such as name, surname, government-issued ID number, date of birth, nationality, gender, ID document details, country of residence, and similar information.
- Contact Details: for example, email address, phone number, residential address.
- User Account Data: such as username, account preferences, etc.
- User Activity Data: including login and session data, usage patterns, activity logs, clickstream data, etc.
- Financial Data: such as bank account details, source of funds, income level, transaction history, and similar information.

- Transaction-Related Data: for example, history and details of transactions made using our services, information regarding the sender and recipient, transaction purpose details, current balance, portfolio details, and other similar data.
- Payment-Related Data: such as bank account details, payment card details, billing address, payment confirmations, etc.
- Employment-Related Data: for example, job title, employment status, employer information, etc.
- Risk-Management Related Data: such as profile of risk, risk level, etc.
- Technical Information and Device-Related Data: for example, IP address, browser type, device type, operating system, data related to interactions with our website, cookies, information about technical issues, etc.
- Communication Preferences: such as your preferences related to marketing.
- Communication-Related Data: including details of user interactions with customer support, records of incoming and outgoing audio calls with the Company.
- Feedback and User Data: such as user feedback, usage patterns and preferences.
- Legal and Regulatory Compliance-Related Data: such as information and documents necessary for compliance with Anti-Money Laundering (AML), Know Your Customer (KYC), and other similar legal and regulatory requirements (including but not limited to identity verification information, proof of address like utility bills, bank statements, etc., photographic evidence like photographs or scans of ID documents, selfies for facial recognition purposes, sanctions and watchlist screening information, etc.
- Claims and Dispute-Related Data: including information about the nature and specifics of the claim or dispute, details about how the claim or dispute was resolved, etc.
- Biometric Identification and Authentication-Related Data: such as facial recognition and fingerprints data, data linked to multi-factor authentication, etc.
- Records and Data Related to On-Site Video Surveillance: including video footage and metadata.

3. PURPOSES AND LEGAL BASES

3.1. General Information

The handling of your personal information by Ventura Payments is guided by explicit and well-defined purposes, each firmly grounded in a lawful basis as required by data protection laws. Our commitment is to ensure the transparent, fair, and purpose-specific processing of your data. In general, the legal bases for processing personal information include:

- Contractual Necessity: Processing that is necessary for the performance of a contract with you or for taking steps at your request before entering into a contract.
- Legal Obligations: Processing of your data to fulfill legal obligations, such as tax or regulatory requirements.
- Legitimate Interests: Processing that is necessary for our legitimate interests or those of a third party, provided your fundamental rights and freedoms do not override those interests.
- Consent: Processing based on your explicit consent, which you can provide when using specific features or services. You retain the right to withdraw your consent at any time.
- Vital Interests: Processing in certain situations to protect your vital interests or those of another person.
- Public Task: Processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

3.2. Detailed Information

To give you a thorough insight into our practices, we have presented an overview of the data processing purposes (namely, reasons for which we collect and process your data) and their respective legal bases (namely, the legal foundations that guide these practices) in the table below.

Data processing purpose	Description	Legal basis
Provision of Services	We process your personal information to support the delivery of our services, which includes handling transactions, overseeing user accounts, and ensuring the functionality and security of our platform.	Contractual Necessity
Legal and Regulatory Compliance	We may process your data to meet legal obligations, such as adhering to financial reporting requirements, complying with anti-money laundering (AML) regulations, and satisfying other legal requirements relevant to our business operations.	Legal Obligation Public Task
Prevention of Fraud	We analyze data to detect and prevent fraudulent activities, safeguarding the security of our services and protecting both users and our business from unauthorized access, misuse, or fraudulent transactions.	Legitimate Interests
Improvement of Services and Troubleshooting	We may process personal data to consistently improve and address any issues with our services. This includes analyzing user interactions, identifying areas for enhancement, and resolving technical issues to ensure a smooth and reliable experience.	Contractual Necessity Legitimate Interests
Management of Risks	Personal data may be processed as part of our comprehensive risk management strategy, which includes assessing and mitigating both operational and business-related risks. This includes analyzing patterns, identifying potential threats, and implementing measures to protect our business operations.	Legal Obligation Legitimate Interests
Security	We may process personal data to ensure the security of our services, incorporating measures for both physical and cyber security. This involves monitoring and preventing unauthorized access, detecting, and preventing fraud, and maintaining the overall integrity of our platform.	Legitimate Interests
Research and Development	Personal data may be processed for research and development purposes, seeking to improve and innovate our	Legitimate Interests

	products and services. This entails analyzing aggregated and anonymized data to identify trends, gain insights, and explore new features.	
Communication and Customer Support	We may process your personal data to offer efficient customer support and facilitate communication with you. This involves addressing inquiries, resolving issues, and delivering crucial service-related information.	Contractual Necessity Legitimate Interests
Marketing	We may process personal data for marketing purposes, with the goal of providing you with relevant information regarding our products, services, promotions, and events. This may encompass personalized content and communications tailored to your preferences, ensuring you remain informed and engaged with our offerings.	Consent Legitimate Interests
Legal Claims and Dispute Resolution	Personal data may be processed when necessary to facilitate the fair and efficient resolution of disputes and legal claims. This involves collecting and analyzing relevant information to assess, address, and potentially settle legal matters.	Legal Obligation Legitimate Interests

4. AUTOMATED DECISIONS AND PROFILING

At Ventura payments, we aim to provide clarity regarding our utilization of automated decision-making processes and profiling techniques to enhance your experience and tailor our services. Here is an overview of these practices:

- **Automated Decision Making:** We may employ automated decision-making processes, including algorithms and machine learning, to improve the efficiency and accuracy of some decisions. These decisions may impact areas such as service eligibility, fraud detection, or risk assessment. Rest assured that we implement appropriate measures to ensure fair and unbiased outcomes, and ensure avenues for human intervention when necessary.
- **Profiling:** Profiling entails the automated processing of personal data to assess, analyze, or predict some aspects related to your preferences, behavior, or interests. This allows us to offer personalized services, recommendations, and targeted communications. Our commitment is to maintain accurate and relevant profiles while respecting your privacy and providing you the ability to manage your preferences.

5. DATA SHARING

At Ventura Payments, safeguarding your privacy is a top priority, and we are dedicated to responsibly sharing your personal data in adherence to applicable laws. Here is an overview of the recipient categories with whom your personal data may be shared:

- **Service Providers:** To ensure the efficient delivery of our services, we may enlist trusted service providers such as payment processors, IT support, and third-party vendors. These entities strictly process your data on our behalf and in accordance with our instructions.

- **Business Partners and Affiliates:** In certain situations, we may share your personal data with our business partners or affiliates. This sharing is conducted in alignment with the purposes outlined in this Privacy Policy and, where required, with your explicit consent.
- **Legal and Regulatory Authorities:** We may disclose your personal data to fulfill legal obligations or respond to lawful requests from governmental or regulatory authorities. This includes situations where disclosure is necessary for the prevention, detection, or investigation of criminal activities.
- **Other Recipients:** With your explicit consent or under another appropriate legal basis, we may share your personal data with third parties for specific purposes not covered by other categories. Should such a case arise, we will ensure that your consent is obtained, or another appropriate legal basis exists before proceeding with such sharing.

6. SECURITY OF INFORMATION

We prioritize the security and confidentiality of your personal information and have implemented a comprehensive set of measures to uphold the integrity and protection of your data. These measures encompass access controls, physical security, data encryption, security audits, incident response, employee training, and other appropriate safeguards. While we employ robust security measures, your active participation in protecting your personal information is equally crucial. We encourage you to adhere to best practices, including using strong and unique passwords, safeguarding login credentials, and exercising caution when sharing information online. Should you have any inquiries about our security practices or suspect unauthorized access, please promptly contact us using the details provided in Section 1. Your cooperation is vital in maintaining the security, privacy of your information, and the overall integrity of our services.

7. YOUR CHOICES AND PREFERENCES

We believe in empowering you with autonomy in managing your personal information. Below are key aspects related to choices available to you regarding the provision of information:

- **Providing Mandatory and Voluntary Information:** Provision of certain information is mandatory for the provision of our services, as required by legal, contractual, or regulatory obligations. Providing this information is essential for service utilization, and without it we will not be able to deliver our services. Where applicable, this information will be marked accordingly.

We may also process optional information that enriches your overall experience and facilitates personalized services tailored to your preferences. Such voluntary information includes information that is not essential for service provision as such but enhances a more individualized interaction. Offering optional information is entirely voluntary and up to your discretion.

- **Editing or Changing Your Information:** You maintain authority over the information you provide. If you hold an account with us, accessing and updating your information is easily achievable through your account settings. For specific requests or assistance, please reach out to us using the contact details in Section 1.
- **Withdrawing Consent:** In cases where we rely on your consent for specific processing activities, such as marketing communications, you possess the right to revoke that consent at any time. Managing your preferences or withdrawing consent can typically be accomplished through provided opt-out mechanisms or by direct contact with us.

8. YOUR RIGHTS

8.1. As an individual, you possess the following rights concerning your personal information:

- **Right to Be Informed:** You have the right to be informed about how we process your information. This Privacy Policy aims to provide transparent details about our data processing practices. For further clarification, please feel free to contact us using the details specified in Section 1 above.

- **Right to Access Your Data:** You can request access to the personal information we have about you.
- **Right to Rectification:** If you believe the personal information we hold about you is inaccurate or incomplete, you can request correction or completion.
- **Right to Erasure:** You have the right to request the deletion of your personal information when it is no longer necessary for the purposes for which it was collected.
- **Right to Restriction of Processing:** You can request processing restriction if you contest the accuracy of personal information, the processing is unlawful, or if we no longer need it for processing purposes.
- **Right to Object:** You can object to the processing of your personal information, except where we have compelling legitimate grounds for the processing.
- **Right to Withdraw Consent:** If your personal data processing relies on your consent, you have the right to withdraw it at any time. Please note that withdrawal doesn't affect the lawfulness of processing before consent withdrawal.
- **Right to Data Portability:** You have the right to receive your provided personal information in a structured, commonly used, and machine-readable format and to transmit it to another controller where technically feasible.

However, it is essential to recognize that these rights are not absolute and may be subject to limitations as prescribed by law.

- 8.2. To exercise your data subject rights, we offer convenient options for you to make requests. You can initiate this process by reaching out to us through the contact details in Section 1 of this Privacy Policy. Additionally, you may find self-help options in your account settings to facilitate specific requests, such as updating your information or managing communication preferences.
- 8.3. For security reasons and to ensure disclosure only to the rightful owner, we may request additional information to verify your identity.

9. INTERNATIONAL TRANSFERS

At Ventura Payments, safeguarding your personal information is our top priority, and we are dedicated to handling it in accordance with applicable data protection laws. Although the majority of our data processing activities take place within Canada and the European Economic Area (EEA), it is crucial to acknowledge that specific situations may require the transfer of your information beyond these regions. Any international transfers of your personal information adhere to relevant data protection laws, incorporating appropriate safeguards and contractual measures to guarantee the ongoing protection of your privacy.

10. RESOLUTION OF COMPLAINTS AND DISPUTES

It is our commitment to promptly and effectively address any concerns or disputes related to the processing of your personal data. If you encounter questions or issues, we encourage you to first contact us using the details provided in Section 1. Our dedicated team will make every effort to collaboratively work with you towards a resolution.

While we recommend reaching out to us initially for fair and equitable solutions to your concerns, you also have the right to file a complaint with the relevant data protection authority. This authority oversees compliance with data protection laws and can independently assess and investigate your complaint. For example, residents of Canada can contact the Office of the Privacy Commissioner of Canada. Whereas residents of the European Union may reach out to the data protection authority of their respective member state. For residents of other countries, we advise contacting your local data protection or privacy regulatory body for guidance on the competent state institution for your specific case.

11. PRIVACY OF CHILDREN

The Company's services are not intended for individuals under the age of 18 (referred to as "Children"). The Company does not knowingly collect personal data from anyone under the age of 18. If you are a parent or guardian and you become aware that your child has provided personal data to the Company, please get in touch with us.

12. CHANGES TO THE PRIVACY POLICY

We reserve the right to periodically update this Privacy Policy. Any revisions will be published on our website, with the date of the latest modification provided. In case of substantial changes, we may, at our discretion, inform you using the contact details we have on record. However, it is your responsibility to regularly review this Privacy Policy to stay informed about how we safeguard your personal information. If you disagree with the modifications, kindly discontinue using our services and reach out to us with any specific concerns you may have.

Effective date: 01.12.2023.