

Privacy Policy

Effective Date 25/10/2023

Primeon Payments Limited Commitment to Privacy

At **Primeon Payments Limited** (also referred to as “Company”, “we”, “our”, or “us”), we are dedicated to maintaining the accuracy, confidentiality, and security of Personal Information. We respect rights under applicable privacy laws and only collect, use, and disclose Personal Information in accordance with those laws. This Privacy Policy outlines how we handle your data when you engage with our range of services and platforms (“Services”) as well as visit our website centaurum.com (“Website”). Please note that this policy does not extend to third-party services or products.

Primeon Payments Limited, incorporated in Canada with registered address at 205-50 LONSDALE AVE NORTH VANCOUVER BC V6M 2E6 CANADA, upholds a strong commitment to protecting your Personal data, irrespective of its processing location or your geographic location.

The [Website](#) may include links to third-party websites (e.g., for event registration purposes). If you visit these third-party websites, please be aware that they have their own privacy policies. We are not responsible for their policies or how they handle your Personal data. It is advisable to review their policies before providing any personal information on these third-party websites.

Data collection procedures

Personal data pertains to information that identifies an individual. In the course of our operations, we employ various methods and ways to gather data:

1. Website

While using our Website, we collect and store the following data:

- Automated technologies like cookies and web beacons to gather browsing information including IP address, browser type, duration of visit, and page views.
- Information provided during your website interaction, such as your full name, email address, phone number, and website.

2. Service

When you use our Services, we may collect, use, store and transfer the following personal data:

- **Information provided directly to the Company:**
The Company collects Personal Information through its Websites (e.g., through cookies), as well as, information directly provided via email, in person, or by phone, including where a person contacts our customer service lines or submits an inquiry.
- **Information received through Primeon Payments Limited merchants, partners and other customers about their customers:**

Primeon Payments Limited may have access to Personal Information that we receive from merchants, partners, and other customers as part of a credit or debit transactions and related value-added services. In the event that you are a merchant seeking to utilize our Services, we shall gather, retain, and handle personal information pertaining to you and any other individuals linked to your application. This may include, but is not limited to, complete names, email addresses, dates of birth, residential addresses, proof of address, copies of personal identification cards or passports, and any additional details necessary for onboarding and compliance with relevant legal regulations.

- ***Collection of Information from third parties:***

We reserve the right to gather personal data from third parties as detailed below.

Payment Processing

If you, as a cardholder, utilize our Services for payment processing to a merchant, we may acquire and process financial and transaction-related personal data directly or through the merchant. This may encompass details such as billing address, delivery address, date of birth, purchase details, payment method, card information, banking details, and any other pertinent data essential for transaction processing.

Compliance Requirements

In adherence to applicable laws, especially anti-money laundering and counter-terrorism financing regulations, we may validate your information and retrieve data from public sources, credit bureaus, fraud prevention agencies, or government sanction lists. This verification process may involve utilizing identity verification providers or due diligence and screening information providers.

Website Security

To secure our website and Services, we may collect information concerning your device, transactions, internet protocol of your computer, and other technical data through our data security and firewall providers.

Marketing Operations

For marketing purposes, we may obtain identity and contact information from publicly available sources to promote our Services effectively. Data usage includes, but is not limited to risk management, fraud prevention, compliance with legal obligations, customer support, and product analysis and improvement.

Usage of Personal data

When serving as your service provider, we may gather, utilize, and reveal specific personal information regarding your customers. It is your duty to ensure that your customers' privacy rights are upheld, which includes providing adequate information regarding third-party data collection and utilization. You are obligated to adhere to the Personal data protection regulations

of your home country and any other countries where you provide goods or services, particularly when handling and transmitting personal data to us in the course of utilizing the Services and conducting transactions. If you have engaged in our Merchant Services Agreement, you are also tasked with meeting the stipulations outlined in the agreement.

In instances where we act as your data processor, we will handle personal data in line with the terms specified in our agreement with you and in accordance with your legal directives.

We will process your Personal data under the following circumstances:

- When it is necessary to execute or fulfill the contract we are entering into or have already entered into with you as our merchant. It is necessary also to provide products and Services (including support) for them.
- When it is essential for our legitimate interests, safeguarding against financial loss or harm to our merchants, yourself, or us, provided that your rights and interests are not overridden.
- When required to adhere to legal or regulatory obligations, such as fraud detection and prevention.
- When necessary for enhancing and analyzing our products, website, systems, and tools.
- When necessary to maintain quality customer Service.
- As otherwise required or permitted by applicable laws and regulations.

Instances of how we may handle your personal data include:

- Responding to inquiries, issuing service notifications, and providing customer assistance.
- Conducting audits, complying with regulatory requirements, and meeting industry standards.
- Notifying you about modifications to the nature or terms of our Service.
- Operating our website, including troubleshooting, data analysis, testing, research, statistical studies, and surveys.
- Enhancing our website to ensure optimal content presentation.
- Verifying your access to your account.
- Enhancing or adjusting our Services.
- Developing new products.
- Distributing marketing communications.
- Performing aggregate analysis and generating business intelligence to enable informed decisions, protect, operate, and report on our business performance.
- Upholding the terms of our website and Services.
- Addressing our daily business requirements, such as monitoring and analyzing operations.
- Anonymizing personal data to provide aggregated statistical information to third parties, such as our clients.
- Safeguarding the website, Services, and you from fraud, abuse, and other illicit activities by monitoring, detecting, and preventing such actions.
- Fulfilling our obligations and enforcing the terms of our website and Services, including compliance with applicable laws and regulations.
- Processing payments, communicating with third parties about payments, and offering associated customer support.
- Detecting illegitimate activities and preventing information security risks associated with our website and Services.

- Assessing your application to utilize our Services and verifying your identity for compliance purposes.

Our practices include risk management, compliance enforcement, payment processing, customer communication, security monitoring, compliance verification, customer support, and continuous service enhancement.

We utilize Personal data to administer our Website effectively, enhance user experience, develop new products, conduct market communications, and generate business intelligence.

Primeon Payments Limited is dedicated to transparent and lawful personal data processing, ensuring a balance between business needs and individual rights.

By leveraging your Personal data for the purposes mentioned above, we strive to enhance the quality of our Services, maintain a secure environment for transactions, and ensure compliance with applicable laws and regulations. Your privacy and data security are paramount to us at Primeon Payments Limited.

Storage and sharing of your Personal data

Your Personal data may be stored and processed within the region of our operational services. By providing us with your personal information, you consent to its transfer, storage, and processing. We employ stringent measures to ensure your data remains secure and confidential. We may share your personal information with the following entities:

1. Service providers
We collaborate with trusted service providers to facilitate operations like data processing, customer support, and fraud prevention.
2. Regulatory bodies
When mandated by law or necessary for compliance, we may share your data with regulatory authorities.
3. Legal obligations
In adherence to legal processes or requests, we may disclose your personal information to law enforcement agencies or judicial bodies.
4. Business transactions
In the event of a merger, acquisition, or sale of assets, your Personal data may be transferred to the acquiring entity.

Disclosure of your Personal data

We disclose your Personal data to trusted third parties in order to provide our Services and advance our business, as outlined below:

- Business partners, payment industry suppliers, and participants in your transactions: we may share your Personal data with our merchants, their service providers, card schemes,

payment method providers, and third-party acquirers as needed to process payments or deliver our Services. This may include:

- Personal data required to facilitate transactions and related activities.
- Personal data to assist partners in resolving disputes, detecting and preventing fraud.
- Personal data and performance analytics to aid merchants in understanding platform usage and enhancing customer experiences.
- Third-party service providers: we may engage third-party service providers to assist us with data and cloud services, website hosting, data analysis, application services, advertising networks, IT infrastructure, customer service, communications, and auditing.
- Advertising and remarketing networks: our Website utilizes remarketing and conversion tracking technologies to display targeted ads to users who have visited our site on partner networks across the internet. Additional providers may be included in the future.
- Other third parties: your Personal data may be shared with third parties in cases of reorganization, merger, sale, joint ventures, transfers, or other business dispositions.
- Safety, Legal Purposes, and Law Enforcement: we may disclose your Personal data to third parties to address fraud, security issues, protect rights, property, safety, or as required by law. This includes enforcement of terms, protection of rights, responses to legal requests, and cooperation with authorities.

All third-party providers and group entities are obliged to process data in compliance with data protection regulations, adhering to Canadian standards and our policies. They are prohibited from using your Personal data for their own purposes. Additionally, when a third party processes your data on our behalf, we establish written agreements outlining security obligations according to Canadian and European data protection laws, limiting data processing to specific purposes.

Retention of the information

Data retention practices are essential to ensure compliance with legal obligations, operational needs, and data security. Retaining data for appropriate durations supports accountability, transparency, and responsible data handling practices. Regular data maintenance and updates play a pivotal role in maintaining the integrity and relevance of stored information.

We retain your Personal data in an identifiable format for the minimum period of five (5) years, this period is necessary to fulfill our legal obligations and business requirements. If permitted by law and within our legitimate interests, we may retain data for extended durations.

Our retention of your Personal data aligns with the purposes for which it was collected, including legal, accounting, or reporting obligations. Factors such as data sensitivity, risk mitigation, processing purposes, and legal requirements influence our retention decisions. In the event of account closure, we reserve the right to retain and access your data as necessary for legal compliance. Cookies utilized on our Website have predefined expiration times, disabling automatically if not revisited within that timeframe, with retained data erased.

Data security and Privacy Protection

Data Security and Privacy Protection are of utmost importance to us. Handling some of your most sensitive information, we have established stringent standards for safeguarding data. Rigorous

security measures are in place to prevent accidental loss, unauthorized access, alteration, or disclosure of your personal data.

To enhance Data Security:

- We restrict access to your personal information to authorized employees and relevant third parties on a need-to-know basis. They handle your data as per our instructions and uphold confidentiality obligations.
- Protocols are implemented to address any suspected data breaches, with notifications sent to you and regulatory bodies where legally required.
- Secure Sockets Layer (SSL) software is utilized to encrypt data during transmission, and information is stored on secure systems.
- Advanced security technologies are employed to thwart unauthorized access to our systems.

Additionally, it is crucial to safeguard your Login ID/password and device against unauthorized access. Ensuring the protection of your access credentials is vital in maintaining security. Data Security measures are vital for maintaining the confidentiality, integrity, and availability of information, safeguarding against unauthorized access, data breaches, and cyber threats.

Right to Access and Correct Personal Information

Your rights under Data protection laws empower you to control and oversee the use of your Personal data. These rights provide transparency and enable you to take charge of how your information is handled by organizations. Data protection regulations aim to protect individuals' privacy and ensure that their data is processed fairly and securely. By utilizing these rights, you can actively manage and safeguard your personal information in an increasingly data-driven world.

Data Protection laws afford you certain rights concerning your Personal data:

1. **Access:** You can request access to your personal data to verify its lawful processing.
2. **Correction:** You have the right to rectify any incomplete or inaccurate personal data we hold.
3. **Erasure:** You can request the deletion of your personal data if no longer necessary for processing or if processed unlawfully.
4. **Objection:** You can object to processing based on legitimate interests or direct marketing, where applicable.
5. **Restriction:** You can request the suspension of data processing in specific scenarios.
6. **Data Portability:** You can request your data in a machine-readable format for transfer.
7. **Withdrawal of Consent:** You can withdraw consent for processing, with exceptions for prior lawful processing.
8. **Request for Manual Review:** If automated decision-making is used, you have the right to contest and request a manual review.

To exercise these rights, contact us at alx@centaurum.com or refer to our website's provided postal address. Once consent is withdrawn, we will cease processing your data for the specified purposes, unless legally justified otherwise.

Transfer of Personal data outside the European Economic Area (EEA)

Primeon Payments Limited is committed to implementing all reasonable legal, technical, and organizational measures to ensure that if your data is transferred outside the EEA, it receives secure treatment with a level of protection equivalent to that within the EEA.

In alignment with European data protection regulations, we have taken specific actions to safeguard your Personal data. We aim to limit data transfers to countries recognized by the European Commission as providing an adequate level of protection for Personal data.

Any transfers of Personal data outside the European region will occur only if the receiving organization has provided us with sufficient safeguards and is bound by a written agreement that complies with European data protection laws governing processors and data transfers.

In cases where you engage with parties outside the EEA, such as transacting with a non-EEA based merchant, utilizing a non-EEA payment method, or using a non-EEA currency, we may need to transfer your Personal data to those parties to fulfill the Services requested.

Links to third-party Websites

While navigating our website, you may encounter links to external third-party websites. These websites, including those required for event registrations, maintain distinct privacy policies for which Primeon Payments Limited bears no responsibility. Prior to disclosing any personal information on these platforms, please review their privacy policies.

Updates to this Privacy Policy

Primeon Payments Limited will update this Privacy Policy from time to time to reflect changes in our Personal Information practices. The information, material and content provided in the pages of the Website may be changed at any time without notice. Changes may be made to the Policy at any time without notice by updating this posting. You agree to review the Policy regularly and your continued access or use of the Website will mean that you agree to any changes.

Questions, Concerns or Complaints

If you have a question, concern or complaint related to this Privacy Policy, Primeon Payments Limited Personal information (including our use of Services outside of your jurisdiction), or wish to exercise applicable rights relating to the collection, use or disclosure of your Personal Information, please contact us via email: alx@centaurum.com