PRIVACY NOTICE

Last Updated: 21 November 2024

INTRODUCTION

Welcome to Guardians of Chain! We are committed to protecting your privacy and safeguarding your personal information. This Privacy Notice ("Notice") outlines the methods by which we collect, use, and protect your data. By using our services or website, you confirm that you have read, understood, and agreed to the terms specified herein. Should you have any questions or require further information, please do not hesitate to contact us. Our dedication to transparency ensures that you are fully informed about our data practices.

ABOUT THE DATA CONTROLLER

Your privacy is of paramount importance to us, and we are committed to ensuring the confidentiality and security of your personal data. Below, you will find the details of our company, which is responsible for managing your data:

1) If you reside in United Kingdom:

Company Name: NUOPLAYM LIMITED
Company Registration No 15858142
Registered Address: 7 Bell Yard, London, England, WC2A 2JR

2) If you reside in EEA:

Company Name: NEONVERSE OÜ
Company Registration No 17108776
Registered Address: Harju maakond, Tallinn, Haabersti linnaosa,Paldiski mnt 199a, 13517

NUOPLAYM LIMITED and NEONVERSE OÜ hereinafter collectively refered to as “we”, “us”, “our” and “Company”, “Data Controller”.

As the Data Controller, we are responsible for determining the purposes and methods by which your personal data is processed. We ensure that all processing activities comply with applicable data protection laws, including the General Data Protection Regulation (GDPR) and the UK GDPR. Our commitment is to handle your data with the utmost responsibility and to safeguard your rights.

Should you have any concerns or require assistance, please do not hesitate to contact us. We are dedicated to providing support and addressing any issues related to your personal data.

CATEGORIES OF PERSONAL DATA COLLECTED

We may collect and utilize the following categories of personal data:

(a) **Account Details:** This encompasses your profile ID, login credentials, activity logs, account settings, photos, avatars, and any other content you choose to share with us.
(b) **Contact Information:** This includes your phone number, email address, and physical address.
(c) **Identity and Authentication Data:** This includes your full name, identification details (such as government-issued ID numbers), details of ID documents, and authentication information.
(d) **Technical Data:** This pertains to device information used to access our services, including IP address, operating system, browser type, and settings.
(e) **Legal Data:** This includes information required for legal compliance, such as Anti-Money Laundering (AML), Counter-Terrorism Financing (CFT), and Know Your Customer (KYC) regulations.
(f) **Customer Support Information:** This involves details of any issues raised, resolution status, and related information.
(g) **Transaction Data:** This consists of order details, purchase history, transaction history, and current balance.

(h) **Payment Information:** This includes payment history, payment status, payment methods, bank account details, and payment card information.
(i) **Communication Data and Logs:** This comprises records of phone calls, chat histories, and email exchanges.
(j) **Marketing Data:** This includes your marketing preferences, participation in loyalty programs, and similar activities.
(k) **On-Site Visitor Data:** This includes video surveillance footage from our premises for security purposes.

Should you have any questions regarding the types of data we collect, please do not hesitate to contact us.

PURPOSES AND LEGAL BASES FOR DATA PROCESSING

We process personal data for various purposes, each supported by specific legal bases:
(a) **Purpose: Service Delivery and Agreement Fulfilment** (Description: Entering into agreements and delivering promised services, ensuring a robust user experience). Legal Basis: Contractual necessity.
(b) **Purpose: Account Creation and Management** (Description: Setting up and managing your user account). Legal Basis: Contractual necessity.
(c) **Purpose: User Identity Verification and Authentication** (Description: Ensuring security and compliance with legal requirements, preventing unauthorized access, and maintaining a secure environment). Legal Basis: Legal obligation, legitimate interests.
(d) **Purpose: Order Fulfilment and Management** (Description: Processing your data to fulfil and manage orders, including transaction processing). Legal Basis: Contractual necessity.
(e) **Purpose: Transaction Processing** (Description: Facilitating transactions, subscriptions, and financial activities, preventing fraud, and ensuring transaction legitimacy). Legal Basis: Contractual necessity, legitimate interests.
(f) **Purpose: Risk Management and Business Decisions** (Description: Managing risks and making informed business decisions, ensuring safety and efficiency via risk assessments and strategic planning). Legal Basis: Contractual necessity, legal obligations, legitimate interests.
(g) **Purpose: Compliance with Legal and Regulatory Requirements** (Description: Ensuring adherence to industry-specific legal requirements, such as KYC, AML regulations, sanctions, and tax obligations). Legal Basis: Legal obligation, public task.
(h) **Purpose: Technical Issue Resolution** (Description: Processing data to troubleshoot and resolve technical issues). Legal Basis: Contractual necessity.
(i) **Purpose: Fraud and Service Misuse Prevention** (Description: Protecting services from fraud and misuse by implementing security measures). Legal Basis: Legal obligation, legitimate interests.
(j) **Purpose: Communication and Customer Support** (Description: Facilitating communication and customer support, ensuring timely assistance). Legal Basis: Contractual necessity, legitimate interests.
(k) **Purpose: Claims Handling and Dispute Resolution** (Description: Processing data for handling claims and resolving disputes). Legal Basis: Contractual necessity, legal obligation, legitimate interests.
(l) **Purpose: Service and Information Security** (Description: Ensuring the security of services and data by safeguarding against unauthorized access, breaches, and other security threats). Legal Basis: Contractual necessity, legal obligation, legitimate interests.
(m) **Purpose: Marketing and Personalized Content** (Description: Delivering personalized marketing materials and content based on preferences). Legal Basis: Consent, legitimate interests.
(n) **Purpose: Service Improvement and Development** (Description: Analysing user feedback and performance metrics to enhance and develop services). Legal Basis: Legitimate interests.

If you have any questions regarding the purposes for processing your data, please contact us. We are committed to transparency and are here to provide clarity on any concerns.

DATA COLLECTION METHODS

We obtain personal data through several channels. This includes direct interactions when you register an account, make purchases, or use our services. Examples of such activities are completing forms, subscribing, and reaching out to customer support.

We also use automated technologies, like cookies and similar tools, to collect data during your interactions with our website (please see our Cookie Notice published on our website for more information on this topic). In

addition, we gather information from third-party sources, such as service partners (e.g., payment processors), government agencies, and public records.

MANDATORY AND OPTIONAL DATA

Certain personal data is required for the proper functioning of our services. If this mandatory data, clearly indicated as such, is not provided, access to specific features may be limited. On the other hand, optional data is not essential and can be adjusted through your account settings. You retain full control over this information and can update it at any time. If you have any questions or need help managing your data, please feel free to contact us for support.

DATA SHARING AND PRIVACY PROTECTION

We do not sell your personal data to third parties. Your data is shared solely for the purposes of fulfilling our service commitments to you, enhancing your experience, and complying with legal obligations. We take every precaution to prevent misuse of your data and to maintain its confidentiality and security.

We may share your data with trusted partners to provide our services and with authorities when legally required. All data sharing is conducted with care and in strict compliance with applicable laws. Our partners include service providers, business partners, and affiliates who assist in delivering and enhancing our services. We ensure these partners uphold the same rigorous standards of data protection that we do.

INTERNATIONAL DATA TRANSFERS

Your personal data may be transferred to countries outside the United Kingdom (UK), the European Economic Area (EEA), and the European Union (EU). We ensure that such transfers comply with data protection laws by implementing robust safeguards, such as Standard Contractual Clauses (SCC) and adhering to adequacy decisions. These measures are designed to provide your data with the same level of protection it would receive within the UK, EEA, and EU.

To further protect your privacy, we take additional steps, such as conducting thorough assessments of our data transfer mechanisms and selecting trusted partners who uphold stringent data protection standards. We are committed to transparency and diligence in managing your personal data across borders.

We regularly review and update our international data transfer practices to ensure ongoing compliance and to safeguard your privacy. Your trust is important to us, and we strive to maintain the highest standards in data protection.

Should you have any questions or require further information regarding the transfer of your data, please do not hesitate to contact us.

DATA STORAGE AND RETENTION

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected or as required by law. Different categories of data have varying retention periods to meet specific legal, operational, and regulatory requirements.

For example, data required to comply with legal obligations, such as information related to Anti-Money Laundering (AML) and sanctions compliance, is typically retained for five years, with possible extensions if mandated by law. This ensures we meet our legal and regulatory duties and can provide accurate reporting and auditing for compliance purposes.

Data relevant to potential legal claims may be kept until the statutory limitation period expires, generally not exceeding ten years. This retention period allows us to defend against any legal claims that may arise within this timeframe.

Once the applicable retention period has expired, we securely delete or anonymize your data to prevent unauthorized access and ensure your privacy. Secure deletion involves permanently erasing the data from our systems, while anonymization means modifying the data so that it can no longer be linked to you.

If you have any questions regarding our data retention practices or need more specific information about the retention periods for particular types of data, please do not hesitate to contact us. We are here to provide clarity and support regarding how your data is managed throughout its lifecycle.

DATA SECURITY

We take the security of your personal data very seriously. Our measures include advanced encryption, stringent access controls, and regular staff training. We employ state-of-the-art security technologies to safeguard your data during transmission and storage. Our access controls ensure that only authorized personnel can access your data. Regular security audits and ongoing staff training keep us updated on the latest data protection best practices.

To further enhance your data security, we recommend the following steps:

- **Use Strong, Unique Passwords:** Ensure your passwords are complex and unique to each of your accounts to prevent unauthorized access.
- **Enable Two-Factor Authentication (2FA):** Adding an extra layer of security can help protect your accounts even if your password is compromised.
- **Be Cautious Online:** Avoid sharing personal information on untrusted websites or through suspicious emails.
- **Regularly Update Software:** Keep your devices and applications up to date to protect against the latest security vulnerabilities.
- **Avoid Public Wi-Fi for Sensitive Transactions:** Use secure, private networks when accessing or transmitting sensitive information.
- **Monitor Your Accounts:** Regularly check your accounts for any suspicious activity and report any concerns immediately.
- **Use Reliable Security Software:** Install and maintain reputable antivirus and anti-malware software on your devices.
- **Be Mindful of Phishing Scams:** Be cautious of unsolicited communications that ask for your personal information or direct you to suspicious websites.

If you have any questions or need further guidance on data protection, please contact us. Together, we can work to ensure your data remains secure. While these steps can significantly enhance your data security, they do not guarantee complete protection. Staying informed and vigilant is key to maintaining your personal data's security.

YOUR DATA SUBJECT RIGHTS

You have the following rights concerning your personal data:

(a) **Right of Access:** You are entitled to request access to your personal data and to receive information on how it is being utilized.
(b) **Right to Rectification:** You can request corrections or updates to any inaccurate or outdated personal data.
(c) **Right to Erasure (Right to be Forgotten):** Under certain circumstances, you can request the deletion of your personal data.
(d) **Right to Restriction of Processing:** You may request that the processing of your personal data be limited in specific situations.
(e) **Right to Object:** You have the right to object to the processing of your personal data for particular purposes, including direct marketing.
(f) **Right to Data Portability:** You can request a copy of your personal data in a machine-readable format or ask for it to be transferred to another data controller.
(g) **Right to Withdraw Consent:** If processing is based on your consent, you can withdraw your consent at any time. Please note that withdrawing consent does not affect the legality of the processing carried out prior to your revocation.

To exercise any of these rights, please feel free to contact us using the information provided. We may need to verify your identity to ensure your data's security. Be aware that these rights are subject to certain legal conditions and limitations, which we will explain upon receiving your request.

Our aim is to provide clarity and support regarding your rights. Should you have any questions or need further assistance, please do not hesitate to reach out to us. We are here to help and ensure you fully understand how your rights are managed in accordance with applicable laws.

AUTOMATED DECISIONS AND PROFILING

We do not engage in automated decision-making that has legal effects. However, we may use profiling to personalize your experience, offering relevant recommendations and enhancing your overall user experience.

AGE RESTRICTIONS

Our services are strictly not intended for individuals under the age of 18. We do not knowingly collect personal data from minors. If you are under 18, you are prohibited from using our services or providing any personal data. Should we discover that we have collected personal data from a minor, we will promptly take all necessary steps to delete such information. If you have reason to believe that we may possess any information from or about a minor, please contact us immediately.

COMPLAINTS AND DISPUTE RESOLUTION

If you have any concerns about our data practices, please reach out to us. We are dedicated to addressing your concerns promptly and effectively. Additionally, if you believe your data protection rights have been violated, you have the right to file a complaint with the relevant supervisory authority.

In the UK, you can contact:

Information Commissioner's Office (ICO)
Wycliffe House, Water Lane, Wilmslow
Cheshire, SK9 5AF
Tel. 0303 123 1113
Email: casework@ico.org.uk
Website: https://ico.org.uk/

In Estonia, you can contact:

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
Tatari 39
10134 Tallinn
Tel. +372 6828 712
Email: info@aki.ee
Website: http://www.aki.ee/

UPDATES TO THE PRIVACY NOTICE

We may periodically update this Notice to reflect changes in our practices or regulatory requirements. The most recent version will always be available on our website. Significant changes will be communicated through appropriate channels, such as email notifications or website alerts.

FURTHER INFORMATION

We respect your privacy and are here to address any questions or concerns about this Privacy Notice or our data practices. For clarification, specific inquiries, or more information, please contact us at info@guardiansofchain.com.