

Privacy Policy of YouGo Limited

1. Introduction

YOUGO LIMITED (“we”, “our”, “the Company”) is committed to respecting your privacy and protecting your personal data. This Privacy Policy explains how we collect, process, store, and safeguard personal information through our online platform, **YouGo**, available at <https://yougo.money>.

This Policy is drafted in accordance with the Personal Data (Privacy) Ordinance (Cap. 486) of the Hong Kong SAR (“PDPO”) and the General Data Protection Regulation (EU 2016/679) (“GDPR”). It applies to all users of the Service, regardless of jurisdiction, with particular emphasis on individuals located in the European Union (EU) and the Hong Kong SAR.

By using our Service, you acknowledge that you have read and understood this Policy and agree to the processing of your data in compliance with the applicable laws.

2. Who We Are

The entity responsible for the collection and processing of your personal data is:

YOUGO LIMITED

Business Registration Number: 78386775-000-06-25-2. Registered Address: Room 602, 6th Floor, Kai Yue Commercial Building, No. 2C Argyle Street, Mong Kok, Kowloon, Hong Kong

We act as the data controller with respect to your personal information, irrespective of whether you are located in the EU, Hong Kong, or elsewhere.

3. What Personal Data We Collect

We may collect and process the following categories of personal data in the course of providing our services:

Identity and Contact Information:

- Full name, date of birth, nationality, gender
- Passport or government-issued ID details
- Tax identification numbers where legally required
- Email address, phone number, residential or business address

Account and Usage Data:

- Login credentials (username/password), user ID
- Browser and device information (IP address, cookies, device type, geolocation)

- Activity logs, access history, and task management data
- User preferences and platform settings

Payment and Financial Information (including crypto):

- Bank account details and billing address
- Cryptocurrency wallet addresses and transaction history
- Credit/debit card information (processed exclusively via certified third-party payment providers in compliance with **PCI DSS**)

Employment and Contractual Data:

- Copies of contracts, invoices, and assignments generated via the platform
- Records of tasks performed, approvals, and payments issued
- Onboarding and verification documents, including AML/KYC results

Media and Verification Data:

- Uploaded identification documents, including photos or scans for verification
- Webcam photos or biometric verification results where required by compliance standards

Other Data:

- Feedback, survey responses, and customer support requests
- Any additional personal data voluntarily submitted by you in the context of using our services

Children's Data:

We do not knowingly collect personal data of individuals under the age of 18, unless such collection is strictly required for lawful contractual arrangements and is in compliance with our Terms of Service and applicable laws.

4. Legal Basis for Processing (Under GDPR)

We only process personal data where a valid legal basis exists under GDPR and PDPO. These include:

- Consent — for optional processing, such as receiving marketing communications.
- Contractual Necessity — to perform our obligations under a service agreement or contract entered into with you.
- Legal Obligation — to comply with applicable laws, including anti-money laundering (AML), counter-terrorist financing (CTF), tax, and financial reporting obligations.
- Legitimate Interests — to ensure security of our platform, improve our services, conduct risk assessments, and prevent fraud, provided that such interests do not override your fundamental rights.

For users in Hong Kong, all collection, use, storage, and processing of personal data are conducted strictly in accordance with the six Data Protection Principles (DPPs) set out in the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO).

This means that:

- Personal data will only be collected for a lawful and necessary purpose directly related to the functions or activities of YUGO LIMITED.
- The data collected will be adequate but not excessive, and used only for the purposes for which it was collected or for directly related purposes.
- We take all reasonably practicable steps to ensure that personal data is accurate, up-to-date, and not retained for longer than necessary.
- Personal data will be stored securely, with access restricted to authorized personnel on a need-to-know basis.
- Individuals are entitled to request access to and correction of their personal data held by us.
- We maintain transparent information about our personal data practices, including the kinds of personal data held, the main purposes of use, and the ways in which data subjects may exercise their rights under the PDPO.

5. How We Use Your Data

We process your personal data exclusively for lawful purposes and in connection with the operation of the YouGo platform, including:

- Account management — to register, authenticate, and maintain your user account.
- Service delivery — to provide access to the platform's core functions, including contractor management, payroll processing, and cross-border payments.
- Support and communications — to provide technical assistance, respond to your requests, and send service-related notices (e.g., policy updates, system alerts).
- Regulatory compliance — to fulfil obligations under applicable laws, including anti-money laundering (AML), counter-terrorist financing (CTF), tax reporting, and labor law requirements.
- Financial processing — to issue invoices, process payments in fiat or digital assets, and maintain accurate financial records.
- Service improvement — to analyze usage trends, enhance functionality, and develop new features.
- Fraud prevention and security — to detect, prevent, and investigate fraudulent activity, unauthorized access, or misuse of the platform.
- Marketing communications — to send information about our services or relevant partner offerings, but only where you have provided explicit consent.

6. Marketing and Consent

We may, from time to time, contact you with marketing communications relating to our services or those of trusted partners. Such communications will only be sent where we have obtained your explicit consent, or where permitted by applicable law.

You have the right to withdraw your consent at any time. Withdrawal of consent will not affect the lawfulness of processing carried out before such withdrawal.

7. Cookies and Tracking Technologies

We use cookies and similar tracking technologies to enhance your user experience and optimize the performance of our Service. These technologies may collect:

- Device identifiers, IP address, and connection type
- Browser type, version, and language settings
- Referring websites or applications
- Pages viewed, interaction logs, and duration of visits

Depending on your jurisdiction, we may rely on either **implied** or **explicit** consent to place cookies. You may manage or disable cookies through your browser or device settings; however, certain features of the Service may not function properly if cookies are disabled.

8. Data Disclosure

We do not sell or otherwise commercially exploit your personal data. We will only disclose personal data to third parties where this is necessary for legitimate business purposes, for the proper provision of our Services, or where disclosure is required or permitted by applicable law or regulation.

In such cases, disclosures may include the following categories of recipients:

- **Affiliates and Group Companies** — We may share information with our affiliates, subsidiaries, or parent company to ensure the effective delivery of our services.
- **Service Providers and Processors** — We may disclose personal data to trusted third-party partners who process data on our behalf, such as IT support, hosting, identity verification providers, and communication services. All such providers are contractually bound by strict confidentiality and data protection obligations, and we only disclose the minimum information necessary for them to provide their services.
- **Auditors, Advisors, and Consultants** — We may disclose information in the context of audits (including external financial, compliance, and security audits) or to professional advisors such as lawyers, accountants, and risk consultants.
- **Regulators, Courts, and Authorities** — We may disclose data to governmental, regulatory, law enforcement, or judicial authorities, where necessary to comply with applicable laws, respond to lawful requests, or enforce our rights.
- **Financial Institutions and Payment Systems** — We may share data with banks, credit institutions, payment networks (e.g., SWIFT, SEPA, Visa, Mastercard), and payment service providers to facilitate legitimate cross-border payments, settlements, and transaction processing.
- **AML/CTF and Risk Prevention Agencies** — Personal data may be disclosed to anti-money laundering (AML), counter-terrorist financing (CTF), fraud prevention, and compliance service providers in order to verify identity, perform due diligence, and ensure lawful use of our platform.

- Cloud and Data Management Providers — We may use secure cloud storage, data archiving, and data management solutions in the ordinary course of business, subject to contractual safeguards.
- Customer Support and Marketing Providers — Where necessary, we may share data with carefully selected third parties assisting us with customer support, marketing communications (subject to consent), and administrative services.
- External Legal Advisors — Where disputes, investigations, or legal proceedings arise, data may be shared with external counsel and advisors.

We may also disclose your data in specific circumstances, including:

- To comply with a legal or regulatory obligation;
- To enforce our contractual rights, investigate breaches, or respond to claims;
- To protect the rights, safety, and property of YOUNGO LIMITED, our clients, or the public;
- To prevent fraud, financial crime, and equivalent risks, including sharing data with relevant companies or organizations for these purposes.

All such disclosures are conducted in accordance with the requirements of the Personal Data (Privacy) Ordinance (PDPO) and the GDPR, ensuring that personal data is protected by appropriate contractual, technical, and organizational safeguards.

9. International Data Transfers

Certain processing activities may require the transfer of your personal data to jurisdictions outside of the Hong Kong SAR or the European Economic Area (EEA). This may include transfers to service providers, financial institutions, or affiliates located in other countries.

Whenever we transfer your personal data internationally, we implement appropriate legal, contractual, and technical safeguards to ensure that your data remains adequately protected. These include:

- Standard Contractual Clauses (SCCs) adopted by the European Commission for transfers from the EEA to third countries;
- Contractual protections under Section 33 of the PDPO, governing the transfer of personal data out of Hong Kong;
- Supplementary technical and organizational measures, such as encryption, access controls, and data minimization, to enhance protection against unauthorized access or misuse.

Where applicable, we will only transfer personal data to jurisdictions that provide an adequate level of data protection or ensure that appropriate safeguards are contractually in place.

You may request further details regarding the safeguards applied to specific international transfers by contacting us at the address set out in Section 15 of this Policy.

10. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes outlined in this Privacy Policy or to comply with applicable legal, regulatory, and contractual obligations. The retention periods may vary depending on the type of data and the requirements of the jurisdictions in which we operate.

In general:

- Account Data — retained for the duration of your active relationship with us and for a period of six (6) months thereafter, unless longer retention is required by law.
- KYC/AML and Verification Records — retained for the minimum period required under applicable anti-money laundering, counter-terrorist financing, and compliance legislation (typically five (5) years from the date of the transaction or termination of the business relationship).
- Financial, Tax, and Contractual Records — retained in accordance with statutory requirements under applicable accounting and tax laws (which may range from five (5) to seven (7) years).
- Technical Logs and Security Data — retained for as long as reasonably necessary to ensure the security and integrity of our systems and to investigate incidents.

When the retention period expires, or where data is no longer required for the purposes described above, we will take appropriate steps to securely delete, anonymize, or irreversibly aggregate the data in accordance with applicable data protection laws.

11. Your Rights

We respect the rights of individuals in relation to their personal data and ensure that such rights may be exercised in accordance with applicable laws, including the General Data Protection Regulation (GDPR) in the European Union and the Personal Data (Privacy) Ordinance (PDPO) in Hong Kong.

If you are in the EU / EEA / UK (under GDPR):

You are entitled to exercise the following rights with respect to your personal data that we process as a controller:

- Right of Access and Portability — You have the right to obtain confirmation as to whether we process your personal data, access such data, and, where technically feasible, request its transfer to another service provider.
- Right to Rectification — You have the right to require us to correct inaccurate or incomplete personal data.
- Right to Erasure — In certain circumstances (e.g., where data is no longer necessary for the original purpose of collection), you may request the deletion of your personal data.

- Right to Restrict Processing — You may request that we suspend processing of your personal data under specific conditions, for example, where you contest the accuracy or legality of the data held.
- Right to Object — You may object to our processing of your personal data in certain circumstances, including for direct marketing purposes.

Please note: the exercise of these rights may not override our obligations under applicable anti-money laundering (AML), counter-terrorist financing (CTF), and financial record-keeping laws. In particular, we may be required to retain certain identification, transaction, or compliance data notwithstanding a request for erasure.

If you are in Hong Kong (under PDPO):

Under the PDPO, you have the following rights:

- Right of Access — You may request confirmation as to whether we hold personal data about you and obtain a copy of such data.
- Right of Correction — You may require us to correct any personal data that is inaccurate or incomplete.
- Right to Transparency — You may request information regarding our personal data practices, including the types of personal data we hold and the purposes of use.
- Right to Withdraw Consent — Where consent is the basis of processing (e.g., for marketing communications), you may withdraw your consent at any time.

Response Times and Fees

- Requests under the GDPR will generally be addressed within 30 calendar days.
- Requests under the PDPO will generally be addressed within 40 calendar days.
- Under Hong Kong law, a reasonable fee may be charged for complying with a data access request.

All requests will be handled in accordance with the applicable legal requirements and subject to verification of identity to protect the security of your data.

12. Data Security

We implement appropriate technical, organizational, and contractual measures to safeguard personal data against unauthorized access, alteration, disclosure, or destruction. These include, without limitation:

- Secure servers, firewalls, and encrypted connections (TLS/HTTPS)
- Encryption of sensitive payment and identification data, including cryptographic wallets and transaction records
- Multi-factor authentication, access controls, and role-based permissions
- Strict password and credential management policies
- Regular vulnerability testing, system monitoring, and intrusion detection
- Confidentiality undertakings and regular training for all personnel with access to personal data

- Vendor due diligence and contractual safeguards with third-party processors

Despite our efforts, no information system or transmission can be guaranteed as fully secure. Users are responsible for maintaining the confidentiality of their login credentials and ensuring secure access to their own devices.

13. Automated Decision-Making

We do not use personal data for automated decision-making that produces legal or similarly significant effects on you. If such processing is ever applied, it will only be carried out where:

- It is necessary for entering into, or the performance of, a contract with you;
- It is expressly authorized by applicable law; or
- It is based on your explicit consent, which may be withdrawn at any time.

In such cases, we will implement measures to safeguard your rights and freedoms, including the right to obtain human intervention and to contest the decision.

14. Updates to This Policy

We may revise this Privacy Policy from time to time to reflect changes in law, regulation, or operational practice. If material changes are made, we will notify you through the Platform, by email, or by other appropriate means.

The most current version of the Privacy Policy will always be available at: <https://yougo.money>.

Your continued use of the Service following the publication of changes constitutes acceptance of the updated Policy.

15. Contact Us

If you have any questions, requests, or concerns regarding this Privacy Policy or the way in which we handle your personal data, you may contact us at:

Email: info@yougo.money

Company: YUGO LIMITED

Business Registration Number: 78386775-000-06-25-2

Registered Office Address: Room 602, 6th Floor, Kai Yue Commercial Building, No. 2C Argyle Street, Mong Kok, Kowloon, Hong Kong

We will review and respond to all legitimate requests in accordance with the applicable requirements of the **GDPR** and the **PDPO**.

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ СЕРВИСА YOUNGO

1. Введение

Компания **YOUNGO LIMITED** («мы», «нас», «Оператор») уважает ваше право на конфиденциальность и принимает на себя обязательство обеспечивать защиту ваших персональных данных. Настоящая Политика конфиденциальности описывает, каким образом мы собираем, обрабатываем, храним и защищаем персональную информацию через нашу онлайн-платформу **YouGo**, доступную по адресу: <https://yougo.money>.

Настоящая Политика составлена в соответствии с требованиями Закона Гонконгского специального административного района о защите персональных данных (Personal Data (Privacy) Ordinance, Cap. 486, далее — PDPO) и Общего регламента ЕС по защите данных (Регламент (ЕС) 2016/679, далее — GDPR). Политика применяется ко всем пользователям Сервиса, независимо от юрисдикции их нахождения, с особым вниманием к пользователям, находящимся в Европейском союзе и в Гонконгском CAP.

Используя наш Сервис, вы подтверждаете, что ознакомились с настоящей Политикой, понимаете её положения и соглашаетесь с использованием ваших персональных данных в соответствии с применимым законодательством.

2. Кто мы

Обработка ваших персональных данных осуществляется компанией:

YOUNGO LIMITED

Business Registration Number: 78386775-000-06-25-2. Зарегистрированный адрес: Room 602, 6th Floor, Kai Yue Commercial Building, No. 2C Argyle Street, Mong Kok, Kowloon, Hong Kong.

Мы являемся юридическим лицом, ответственным за обработку ваших персональных данных, независимо от того, находитесь ли вы в Европейском союзе, в Гонконге или в иной юрисдикции.

3. Какие персональные данные мы собираем

Мы можем собирать и обрабатывать следующие категории персональных данных в связи с использованием вами сервиса **YouGo**:

Идентификационная информация:

- Полное имя, дата рождения, гражданство, пол;
- Паспортные данные или реквизиты иного удостоверяющего документа;
- Идентификационные номера (например, налоговый номер, где это требуется законодательством).

Контактные данные:

- Адрес электронной почты, номер телефона, почтовый или фактический адрес проживания;
- Данные о месте работы и должности (для корпоративных пользователей).

Данные учетной записи и использования:

- Учетные данные (логин и пароль), идентификатор пользователя;
- Информация о браузере и устройстве (например, IP-адрес, cookies, тип устройства, язык интерфейса);
- Журналы активности и история авторизаций;
- Настройки и пользовательские предпочтения.

Платежная и финансовая информация:

- Банковские реквизиты (номер счета, реквизиты получателя);
- Адрес для выставления счетов;
- Реквизиты криптовалютных кошельков и история транзакций;
- Данные кредитных/дебетовых карт (обрабатываются исключительно через сертифицированных сторонних провайдеров в соответствии с требованиями PCI DSS).

Медиа и данные для верификации:

- Фото или видео с веб-камеры, а также загруженные документы, используемые для идентификации и KYC/AML-проверок;
- Результаты биометрической или иной проверки личности (при необходимости).

Иное:

- Отзывы, ответы на опросы, переписка со службой поддержки;
- Любая дополнительная информация, которую вы добровольно предоставляете в процессе использования сервиса.

Дети:

Мы не осуществляем преднамеренный сбор персональных данных лиц младше 18 лет, за исключением случаев, когда такой сбор прямо предусмотрен условиями использования сервиса **YouGo** и разрешен применимым законодательством.

4. Правовые основания для обработки (в соответствии с GDPR и PDPO)

Мы обрабатываем персональные данные только на законных основаниях, включая:

- **Согласие** — при использовании необязательных функций (например, при получении маркетинговых материалов или участии в опросах).
- **Необходимость для исполнения договора** — для предоставления доступа к Сервису, исполнения обязательств по договору и обеспечения корректного функционирования платформы.
- **Юридическая обязанность** — в случаях, когда обработка персональных данных прямо требуется законом (например, для целей противодействия отмыванию доходов, финансированию терроризма, ведения налоговой и бухгалтерской отчётности).
- **Законные интересы** — для обеспечения безопасности Сервиса, предотвращения мошенничества, проведения анализа и улучшения пользовательского опыта, при условии, что такие интересы не нарушают ваши основные права и свободы.

Для пользователей из Гонконга все действия по сбору и обработке персональных данных осуществляются в соответствии с шестью Принципами защиты данных (Data Protection Principles, DPPs), изложенными в PDPO.

5. Как мы используем ваши данные

Ваши персональные данные используются нами исключительно для законных целей, включая:

- Регистрацию и аутентификацию учётной записи;
- Обеспечение функционирования и поддержания работоспособности Сервиса;
- Предоставление технической помощи и ответов на ваши запросы;
- Выполнение требований законодательства и регуляторных органов (AML, CTF, налоговое регулирование, валютный контроль);
- Отправку служебных уведомлений (например, изменения в политике или системные сообщения);
- Отправку маркетинговых материалов (только при наличии вашего явного согласия);
- Улучшение качества сайта, сервисов и продуктов на основе анализа поведения пользователей;
- Обнаружение, предотвращение и расследование случаев мошенничества, нарушений безопасности или злоупотреблений.

6. Маркетинг и согласие

Мы можем направлять вам маркетинговые сообщения о наших продуктах, сервисах или специальных предложениях от наших доверенных партнёров.

Любая маркетинговая коммуникация осуществляется только при наличии вашего явного согласия.

Вы имеете право в любой момент отозвать согласие на получение таких материалов, воспользовавшись функцией «Отписаться» в электронном письме или связавшись с нами напрямую по контактам, указанным в разделе 15 настоящей Политики.

7. Cookies и технологии отслеживания

Для улучшения качества предоставляемых услуг и персонализации пользовательского опыта мы используем cookies и аналогичные технологии отслеживания. Эти технологии могут собирать следующую информацию:

- IP-адрес и тип устройства;
- Тип и версия браузера;
- Настройки языка;
- Источник перехода (реферер);
- Посещённые страницы и длительность сессии.

Использование cookies осуществляется на основании вашего явного или подразумеваемого согласия в зависимости от применимой юрисдикции. Вы можете изменить или ограничить использование cookies в настройках вашего браузера, однако это может повлиять на корректность работы некоторых функций Сервиса.

8. Раскрытие данных

Мы не передаём ваши персональные данные третьим лицам, за исключением случаев, когда это необходимо для:

- законных бизнес-интересов YUGO LIMITED;
- исполнения договорных обязательств;
- предоставления запрашиваемых вами услуг;
- соблюдения требований законодательства и регуляторов.

В таких случаях раскрытие персональных данных может включать следующие категории получателей:

- **Аффилированные лица и дочерние компании** — для обеспечения централизованного управления и предоставления услуг.
- **Поставщики услуг и процессоры** — сторонние партнёры, которые обрабатывают данные от имени YUGO LIMITED (например, провайдеры ИТ-решений, хостинг, облачные сервисы, коммуникации, техническая поддержка). Все такие партнёры обязаны соблюдать договорные обязательства по конфиденциальности и защите данных.
- **Аудиторы, консультанты и советники** — в целях проведения финансовых, юридических, регуляторных или ИТ-аудитов, а также для расследования инцидентов, связанных с безопасностью и рисками.
- **Регуляторы, суды и правоохранительные органы** — при исполнении требований законодательства, по запросу государственных органов или на основании судебных решений.

- **Финансовые учреждения и платёжные системы** — банки, кредитные организации, SWIFT, SEPA, Visa, Mastercard и другие платёжные провайдеры, необходимые для проведения транзакций.
- **AML/CTF и службы предотвращения мошенничества** — агентства и провайдеры, участвующие в проверке личности, управлении рисками и соблюдении законодательства по борьбе с отмыванием денег и финансированием терроризма.
- **Клиентская поддержка и маркетинг** — подрядчики, обеспечивающие коммуникации с клиентами и управление маркетинговыми кампаниями (только при наличии вашего согласия).
- **Административные, бухгалтерские и юридические консультанты** — для исполнения обязательств в сфере корпоративного управления и соответствия требованиям законодательства.

Мы также можем раскрывать персональные данные в исключительных случаях, если это необходимо для:

- выполнения обязанностей по закону или по регуляторному требованию;
- защиты прав, собственности или безопасности YOUGO LIMITED, наших клиентов или третьих лиц;
- предотвращения мошенничества, финансовых преступлений и аналогичных рисков.

9. Международная передача данных

Некоторые из наших партнёров и поставщиков услуг могут находиться за пределами **Гонконга** и **Европейской экономической зоны (ЕЭЗ)**. В таких случаях мы обеспечиваем надлежащий уровень защиты ваших персональных данных с использованием следующих механизмов:

- **Типовые договорные положения (Standard Contractual Clauses, SCCs)**, утверждённые Европейской комиссией, — для передачи данных из ЕЭЗ в третьи страны.
- **Договорные механизмы, соответствующие Разделу 33 PDPO** — для трансграничной передачи данных из Гонконга.
- **Дополнительные технические и организационные меры безопасности** — такие как шифрование, ограничение доступа и анонимизация, чтобы минимизировать риски при международной передаче данных.

Вы имеете право запросить дополнительные сведения о применяемых гарантиях и механизмах защиты, обратившись к нам по контактам, указанным в разделе 15 настоящей Политики.

10. Сроки хранения данных

Мы храним ваши персональные данные только в течение периода, необходимого для достижения целей, указанных в настоящей Политике, либо для исполнения юридических и договорных обязательств. Конкретные сроки зависят от категории данных и требований законодательства.

Как правило:

- **Данные аккаунта** — хранятся в течение срока вашего пользования Сервисом плюс шесть (6) месяцев после прекращения отношений.
- **Данные KYC/AML и верификации** — хранятся не менее пяти (5) лет после завершения деловых отношений или совершения транзакции в соответствии с обязательными требованиями по противодействию отмыванию доходов и финансированию терроризма.
- **Финансовая, налоговая и бухгалтерская документация** — хранится в течение сроков, установленных применимым законодательством (как правило, от пяти (5) до семи (7) лет).
- **Журналы безопасности и технические записи** — хранятся столько, сколько это необходимо для обеспечения безопасности, мониторинга и расследования инцидентов.

По окончании установленных сроков хранения данные подлежат безопасному удалению, анонимизации или агрегированию, исключающему возможность восстановления личности субъекта данных.

11. Ваши права

Мы уважаем ваши права в отношении персональных данных и обеспечиваем их реализацию в соответствии с применимым законодательством, включая Общий регламент по защите данных (GDPR) и Закон Гонконгского САР о защите персональных данных (PDPO).

Если вы находитесь в ЕС/ЕЭЗ/Швейцарии/Великобритании (GDPR):

Вы обладаете следующими правами:

- **Право на доступ и переносимость данных** — вы имеете право получить доступ к вашим персональным данным и, при определённых условиях, запросить их предоставление в формате, пригодном для передачи другому провайдеру услуг.
- **Право на исправление** — вы имеете право требовать от нас корректировки неточных или неполных данных.
- **Право на удаление данных («право быть забытым»)** — вы можете требовать удаления ваших персональных данных в случаях, когда они больше не нужны для целей обработки или обработка является неправомерной.
- **Право ограничить обработку** — вы можете требовать временного ограничения обработки ваших данных, например, если оспариваете их точность или правомерность обработки.

- **Право возражать против обработки** — вы можете возразить против обработки персональных данных в определённых случаях, включая использование данных для целей прямого маркетинга.

При этом, реализация вышеуказанных прав не освобождает нас от исполнения обязанностей по хранению данных в соответствии с обязательными требованиями законодательства по противодействию отмыванию доходов (AML/CTF) и финансовой отчётности.

Если вы находитесь в Гонконге (PDPO):

Вы обладаете следующими правами:

- Запросить доступ к вашим персональным данным, находящимся у нас;
- Потребовать исправления неточных или неполных данных;
- Получить информацию о целях и практике обработки ваших данных;
- Отозвать согласие на необязательную обработку (например, на маркетинговые рассылки).

Мы стремимся отвечать на запросы субъектов данных в установленные законом сроки: до 30 календарных дней (GDPR) и до 40 календарных дней (PDPO).

В соответствии с законодательством Гонконга мы вправе взимать разумную плату за обработку запросов на доступ к данным.

12. Защита данных

Мы применяем соответствующие технические, организационные и правовые меры для защиты персональных данных от несанкционированного доступа, изменения, раскрытия или уничтожения. В частности, мы используем:

- Безопасные серверы, межсетевые экраны и шифрованные соединения (TLS/HTTPS);
- Шифрование чувствительных данных, включая платёжные реквизиты и криптовалютные транзакции;
- Контроль доступа, основанный на ролях, и многофакторную аутентификацию;
- Политику надёжных паролей и регулярную смену ключей доступа;
- Постоянный мониторинг систем, ведение журналов безопасности и использование средств обнаружения вторжений;
- Регулярное тестирование на уязвимости и независимые аудиты информационной безопасности;
- Обязательные соглашения о конфиденциальности и обучение сотрудников правилам защиты данных и AML/CTF-комплаенсу;
- Контроль подрядчиков и третьих лиц через договорные обязательства по обеспечению безопасности и конфиденциальности данных.

Несмотря на принятые меры, мы не можем гарантировать абсолютную защиту информации в сети Интернет. Вы также несёте ответственность за сохранность своих учётных данных и обеспечение безопасности доступа к собственным устройствам и криптографическим ключам.

13. Автоматизированные решения

Мы не используем механизмы автоматизированной обработки персональных данных для принятия решений, имеющих юридические последствия или иным образом существенно влияющих на ваши права, за исключением следующих случаев:

- **Необходимость для исполнения договора** — например, автоматическая генерация счетов или договоров в рамках использования Сервиса;
- **Предусмотрено законом** — если такая обработка прямо установлена нормативными актами;
- **Явное согласие** — если вы прямо предоставили согласие на использование автоматизированных инструментов (например, при настройке определённых функций платформы).

В случаях, когда применяется автоматизированная обработка, мы гарантируем реализацию ваших прав, включая возможность получения человеческого вмешательства, выражения своей позиции и оспаривания принятого решения.

14. Обновления Политики

Мы можем периодически обновлять настоящую Политику конфиденциальности в связи с изменениями законодательства, регуляторных требований или нашей операционной деятельности.

В случае внесения существенных изменений мы уведомим вас посредством публикации обновления в Сервисе, отправки электронного письма либо через другие доступные каналы связи.

Актуальная версия Политики всегда будет доступна на нашем официальном сайте: <https://yougo.money>.

Продолжение использования Сервиса после публикации изменений будет рассматриваться как подтверждение вашего согласия с обновлённой редакцией Политики.

15. Контактная информация

Если у вас есть вопросы, запросы или жалобы, связанные с настоящей Политикой конфиденциальности или практикой обработки персональных данных, вы можете связаться с нами:

Email: info@yougo.money

Компания: YOUGO LIMITED

Business Registration Number: 78386775-000-06-25-2

Зарегистрированный адрес: Room 602, 6th Floor, Kai Yue Commercial Building,
No. 2C Argyle Street, Mong Kok, Kowloon, Hong Kong

Мы рассмотрим ваш запрос и предоставим ответ в сроки, установленные применимым законодательством (30 календарных дней — GDPR, 40 календарных дней — PDPO).