PRIVACY POLICY

Company Information:
PAYMENT ASSIST LTD
Company Registration Number: 08752986
Registered Address: Pera Business Park, Nottingham Road, Melton Mowbray, Leicestershire, England, LE13 0PB

INTRODUCTION

PAYMENT ASSIST LTD ("Company," "we," "us," or "our") is committed to protecting and respecting your privacy in accordance with applicable data protection laws and regulations. This Privacy Policy ("Policy") describes how we collect, use, process, store, share, and protect personal information and data when you access, visit, browse, or use the Snap Wallet platform, website, mobile applications, and related services (collectively, the "Platform").

This Policy applies to all users, visitors, and individuals who interact with the Platform in any capacity ("you," "your," or "User"). By accessing or using the Platform, you acknowledge that you have read, understood, and agree to the practices described in this Privacy Policy. If you do not agree with this Policy, you must not access or use the Platform.

This Privacy Policy should be read in conjunction with our Terms of Service and any other policies or notices we may provide to you from time to time. Where the Terms of Service conflict with this Privacy Policy, the Terms of Service shall prevail to the extent of such conflict.

We reserve the right to modify, update, or amend this Privacy Policy at any time in our sole discretion. Any changes will become effective immediately upon posting the revised Policy on the Platform. Your continued use of the Platform after changes are posted constitutes your acceptance of the revised Policy. We encourage you to review this Policy regularly to stay informed about our information practices.

---

1. INFORMATION WE COLLECT

1.1 Personal Identification Information

We collect various types of personal information that can directly or indirectly identify you as an individual, including but not limited to:

(a) **Identity Data:** Full legal name, username, maiden name, aliases, date of birth, age, gender, marital status, nationality, citizenship status, country of residence, passport number, passport expiration date, national identity card number, driver's

license number, social security number (where applicable), tax identification number, photographs, and any other government-issued identification information;

(b) **Contact Data:** Residential address, mailing address, billing address, shipping address, email address (personal and business), telephone numbers (mobile, home, work), fax numbers, emergency contact information, and any other contact details you provide;

(c) **Account Data:** Username, user ID, account number, password, security questions and answers, authentication credentials, biometric data used for authentication (such as fingerprints or facial recognition data), account preferences, profile information, security settings, notification preferences, and any other information associated with your account;

(d) **Verification and KYC Data:** Documents and information collected for identity verification, Know Your Customer (KYC) procedures, anti-money laundering (AML) compliance, source of funds verification, proof of address documents, utility bills, bank statements, employment information, income verification documents, and any other verification materials;

(e) **Demographic Information:** Age range, income level, education level, occupation, employment status, employer name and address, job title, professional qualifications, family size, household composition, and other demographic characteristics.

1.2 Financial and Transaction Information

We collect comprehensive financial information necessary for processing payments and transactions, including:

(a) **Payment Instrument Data:** Credit card numbers, debit card numbers, card expiration dates, card verification values (CVV/CVC), cardholder names, billing addresses associated with cards, bank account numbers, bank routing numbers, IBAN numbers, SWIFT/BIC codes, payment processor account information (PayPal, Stripe, etc.), cryptocurrency wallet addresses, and any other payment method details;

(b) **Transaction Data:** Transaction history, payment amounts, payment dates and times, payment status, transaction descriptions, merchant information, invoice numbers, order numbers, purchase history, refund history, chargeback information, dispute records, and complete records of all financial transactions conducted through the Platform;

(c) **Financial Profile Data:** Credit scores, credit history, creditworthiness assessments, financial statements, asset information, liability information,

investment portfolios, net worth estimates, spending patterns, and any other financial profile information;

(d) **Taxation Information:** Tax identification numbers, VAT numbers, tax residence information, tax withholding details, tax forms and documentation, and information necessary for tax reporting and compliance.

1.3 Technical and Device Information

We automatically collect technical information about your devices, systems, and interactions with the Platform, including:

(a) **Device Information:** Device type, device model, device manufacturer, device identifiers (UDID, IMEI, serial numbers), operating system and version, mobile network information, device settings, hardware specifications, screen resolution, battery level, available storage space, installed fonts, and other device characteristics;

(b) **Connection Information:** IP addresses (both IPv4 and IPv6), MAC addresses, Internet Service Provider (ISP) information, connection type (WiFi, cellular, etc.), connection speed, network status, proxy server information, and other connection-related data;

(c) **Browser and Application Data:** Browser type and version, browser language settings, browser plugins and extensions, user agent strings, referring/exit pages, URLs accessed, page response times, download errors, length of visits to pages, page interaction information, application version, application settings, and crash reports;

(d) **Log Data:** Server logs, access logs, error logs, security logs, timestamps of activities, IP addresses accessing the Platform, pages viewed, time spent on pages, click data, scroll depth, forms submitted, download activity, upload activity, and other system-generated log information;

(e) **Cookies and Tracking Technologies Data:** Information collected through cookies, web beacons, pixels, tags, scripts, local storage, session storage, and other tracking technologies, including cookie IDs, tracking IDs, session IDs, and related metadata.

1.4 Location Information

We collect various types of location data, including:

(a) **Precise Location Data:** GPS coordinates, latitude and longitude, altitude, speed, direction of travel, and real-time location tracking data when you enable location services on your device;

(b) **Approximate Location Data:** Location derived from IP addresses, WiFi access points, cell tower triangulation, and other network-based location technologies;

(c) **Location History:** Historical records of places you have been, frequency of visits to locations, time spent at locations, routes traveled, and patterns of movement;

(d) **Geographic Preferences:** Preferred locations, home and work addresses, saved places, favorite locations, and other location-based preferences.

1.5 Usage and Behavioral Information

We collect detailed information about how you use and interact with the Platform, including:

(a) **Platform Usage Data:** Features and functionalities accessed, services used, pages visited, sections explored, content viewed, searches performed, search queries entered, filters applied, sort preferences, navigation paths, user flows, session duration, frequency of visits, time of day usage patterns, and feature adoption metrics;

(b) **Interaction Data:** Clicks, taps, swipes, scrolls, hovers, form field interactions, button presses, menu selections, drag-and-drop actions, copy-paste activities, keyboard inputs, voice inputs, gestures, and all other forms of interaction with the Platform;

(c) **Content Creation and Submission Data:** Messages sent, comments posted, reviews written, ratings provided, feedback submitted, support tickets created, forms filled out, files uploaded, images uploaded, videos uploaded, and any other content created or submitted through the Platform;

(d) **Preferences and Settings:** Language preferences, display preferences, theme selections (light/dark mode), notification settings, privacy settings, communication preferences, accessibility settings, time zone settings, currency preferences, and all other user-configured settings;

(e) **Behavioral Patterns:** Usage patterns, behavior patterns, activity patterns, engagement levels, feature usage frequency, session patterns, conversion patterns, abandonment patterns, and other behavioral analytics.

1.6 Communications and Correspondence

We collect and retain records of all communications and interactions, including:

(a) **Direct Communications:** Emails sent to us, messages sent through Platform messaging systems, customer support inquiries and tickets, live chat conversations,

phone call recordings (where permitted by law), voicemail messages, SMS/text messages, social media messages, and any other direct communications;

(b) **Marketing Communications:** Responses to surveys, responses to polls, participation in contests or promotions, feedback on marketing campaigns, email open rates, email click rates, marketing engagement metrics, and communication preferences;

(c) **Metadata:** Email headers, sender and recipient information, timestamps, subject lines, attachment information, message sizes, delivery status, read receipts, and other communication metadata.

1.7 Social Media and Third-Party Information

When you interact with us through social media platforms or connect third-party services, we may collect:

(a) **Social Media Profile Data:** Social media usernames, profile pictures, profile URLs, public profile information, friends/followers lists, social media posts and activity, likes and interests, and any information you choose to share from your social media accounts;

(b) **Third-Party Service Data:** Information from third-party services you connect to the Platform, including authentication information, profile data, permissions granted, linked account information, and data shared through APIs;

(c) **Social Login Information:** When you use social login features (e.g., "Sign in with Google," "Login with Facebook"), we receive information authorized by you from those platforms, including email address, name, profile picture, and other information you permit.

1.8 Automatically Collected Information

In addition to information you provide directly, we automatically collect information through various technologies, including:

(a) Information collected through cookies, web beacons, pixels, and similar tracking technologies;

(b) Analytics information collected by analytics services and tools we use (such as Google Analytics, Mixpanel, Amplitude, etc.);

(c) Information collected through software development kits (SDKs) and application programming interfaces (APIs);

(d) Metadata associated with files, documents, and content you upload or transmit;

(e) Information collected through heatmaps, session recordings, and user experience tools;

(f) Crash reports, error logs, performance metrics, and diagnostic information;

(g) Information about other devices, applications, and networks you use to access the Platform.

1.9 Information from Third-Party Sources

We may receive information about you from various third-party sources, including:

(a) **Data Brokers and Data Aggregators:** Demographic information, consumer behavior data, interest categories, lifestyle information, purchasing behavior, and other commercially available data;

(b) **Credit Bureaus and Financial Institutions:** Credit reports, credit scores, financial history, account verification information, and fraud detection information;

(c) **Identity Verification Services:** Identity verification results, document authentication results, biometric verification results, fraud risk assessments, and compliance screening results;

(d) **Marketing Partners and Affiliates:** Referral source information, campaign attribution data, lead information, and marketing performance data;

(e) **Public Sources:** Publicly available information from government databases, public records, social media platforms, business directories, professional networking sites, news articles, and other public sources;

(f) **Business Partners and Service Providers:** Information from companies we partner with to provide services, including payment processors, fraud prevention services, analytics providers, and customer support platforms.

1.10 Inferred and Derived Information

Based on the information we collect, we may create, derive, or infer additional information about you, including:

(a) **User Profiles and Segments:** Demographic profiles, psychographic profiles, behavioral segments, interest categories, propensity models, and predictive attributes;

(b) **Risk and Fraud Scores:** Fraud risk scores, creditworthiness assessments, trust scores, security risk assessments, and other risk-related metrics;

(c) **Preferences and Interests:** Inferred preferences, predicted interests, product recommendations, content recommendations, and personalization attributes;

(d) **Analytics and Insights:** Usage patterns, engagement metrics, lifetime value estimates, churn probability, conversion likelihood, and other analytical insights.

---

2. HOW WE USE YOUR INFORMATION

2.1 Primary Purposes

We use the personal information we collect for various purposes, including but not limited to:

(a) **Platform Operation and Service Delivery:**

- Operating, maintaining, administering, and managing the Platform and its features;
- Providing, delivering, and performing the services described on the Platform, to the extent such services are operational;
- Creating, managing, and maintaining user accounts;
- Authenticating users and verifying identities;
- Processing registrations and account setup;
- Enabling platform functionality and features;
- Responding to user requests and inquiries;
- Providing customer support and technical assistance;
- Troubleshooting technical problems and resolving issues;
- Monitoring platform performance, uptime, and availability.

(b) **Transaction Processing and Financial Operations:**

- Processing payments, contributions, and financial transactions;
- Verifying payment information and payment methods;
- Managing billing and invoicing processes;
- Processing refunds, adjustments, and chargebacks (where applicable);
- Maintaining transaction records and financial histories;
- Reconciling accounts and financial reporting;
- Conducting financial analysis and forecasting;
- Managing revenue and financial operations.

(c) **Identity Verification and Compliance:**

- Verifying user identity and conducting Know Your Customer (KYC) procedures;
- Performing anti-money laundering (AML) checks and screenings;

- Conducting sanctions screening and watchlist checks;
- Verifying source of funds and source of wealth;
- Ensuring compliance with legal and regulatory requirements;
- Maintaining compliance records and documentation;
- Responding to regulatory inquiries and audits;
- Meeting reporting obligations to authorities.

(d) **Security, Fraud Prevention, and Risk Management:**

- Detecting, preventing, and investigating fraud, unauthorized access, and security breaches;
- Monitoring for suspicious activity and security threats;
- Implementing security measures and access controls;
- Conducting risk assessments and risk management;
- Protecting against malicious, deceptive, fraudulent, or illegal activity;
- Investigating violations of our Terms of Service;
- Enforcing our policies, terms, and agreements;
- Protecting our rights, property, and safety, and the rights, property, and safety of users and third parties.

2.2 Communication and Engagement

We use your information to communicate with you and engage with you through various channels:

(a) **Operational Communications:**

- Sending account-related notifications and alerts;
- Providing transaction confirmations and receipts;
- Sending security alerts and important notices;
- Notifying you of changes to the Platform, services, or policies;
- Sending password reset and account recovery communications;
- Delivering system updates and maintenance notifications;
- Providing customer support communications and responses.

(b) **Marketing and Promotional Communications:**

- Sending marketing emails, newsletters, and promotional materials;

- Providing information about new features, services, and offerings;
- Delivering targeted advertising and personalized marketing;
- Conducting surveys, polls, and market research;
- Sending invitations to events, webinars, and promotions;
- Delivering product recommendations and suggestions;
- Promoting special offers, discounts, and incentives.

(c) **Transactional Communications:**

- Confirming orders, registrations, and subscriptions;
- Providing status updates on transactions and activities;
- Sending invoices, statements, and billing information;
- Notifying you of payment successes or failures;
- Providing receipts and transaction documentation.

2.3 Platform Improvement and Development

We use your information to improve, develop, and enhance the Platform:

(a) **Analytics and Research:**

- Analyzing usage patterns, trends, and behaviors;
- Conducting research and development activities;
- Gathering insights about user preferences and needs;
- Performing statistical analysis and data modeling;
- Identifying opportunities for improvement and innovation;
- Measuring platform performance and effectiveness;
- Benchmarking against industry standards and competitors.

(b) **Product Development and Testing:**

- Developing new features, functionalities, and services;
- Testing new concepts, designs, and technologies;
- Conducting A/B testing and multivariate testing;
- Gathering user feedback on prototypes and beta features;
- Iterating on product designs based on user behavior;
- Optimizing user experience and interface design;

- Enhancing platform usability and accessibility.

(c) **Personalization and Customization:**

- Personalizing content, features, and experiences for individual users;
- Customizing recommendations and suggestions;
- Tailoring marketing messages and offers;
- Adapting platform interface based on preferences;
- Creating personalized user journeys and experiences;
- Providing relevant content and information.

2.4 Business Operations and Administration

We use your information for various business and administrative purposes:

(a) **Business Management:**

- Managing business operations and internal processes;
- Conducting financial planning and analysis;
- Preparing financial reports and statements;
- Managing vendor and partner relationships;
- Conducting business development activities;
- Evaluating business performance and metrics;
- Making strategic business decisions.

(b) **Legal and Compliance:**

- Complying with legal obligations and regulatory requirements;
- Responding to legal processes, subpoenas, and court orders;
- Defending against legal claims and litigation;
- Maintaining legal and compliance records;
- Conducting internal audits and investigations;
- Ensuring adherence to industry standards and best practices;
- Managing intellectual property rights.

(c) **Corporate Transactions:**

- Evaluating, negotiating, and completing mergers, acquisitions, or sales of assets;

- Conducting due diligence for business transactions;
- Transferring information in connection with corporate reorganizations;
- Managing investments and financing activities;
- Facilitating business continuity and succession planning.

2.5 Demonstration and Research Purposes

Given the demonstrative nature of the Platform as described in our Terms of Service, we may use your information for:

(a) Demonstrating platform capabilities and functionalities to potential partners, investors, or stakeholders;

(b) Conducting market research and feasibility studies;

(c) Testing and evaluating technological concepts and innovations;

(d) Gathering feedback on user interface designs and user experiences;

(e) Analyzing market demand and user interest in potential services;

(f) Creating case studies, reports, and presentations (with anonymization where appropriate);

(g) Benchmarking performance metrics and key performance indicators;

(h) Validating business models and strategic directions.

2.6 Aggregated and De-identified Data

We may aggregate, anonymize, or de-identify your personal information so that it can no longer reasonably be used to identify you. We may use such aggregated, anonymized, or de-identified data for any purpose, including:

(a) Creating statistical analyses, reports, and insights;

(b) Conducting research and analysis on industry trends;

(c) Developing and improving algorithms and models;

(d) Sharing insights with partners, clients, or the public;

(e) Benchmarking and comparative analysis;

(f) Creating datasets for machine learning and artificial intelligence purposes;

(g) Publishing research papers, articles, and thought leadership content.

2.7 Other Purposes

We may also use your information for other purposes that are:

(a) Disclosed to you at the time of collection;

(b) Related to the purposes described in this Policy;

(c) Required or permitted by applicable law;

(d) Necessary to protect our legitimate interests;

(e) Consented to by you;

(f) Otherwise reasonably expected given the context of collection.

---

3. LEGAL BASIS FOR PROCESSING

Where applicable under data protection laws (such as the General Data Protection Regulation - GDPR), we process your personal information based on one or more of the following legal grounds:

3.1 Consent

We process your personal information based on your explicit consent where:

(a) You have provided clear, affirmative consent for specific processing activities;

(b) You have opted in to receive marketing communications;

(c) You have agreed to the use of cookies and tracking technologies;

(d) You have authorized the processing of special categories of data;

(e) Processing is required by law to be based on consent.

You have the right to withdraw your consent at any time, without affecting the lawfulness of processing based on consent before withdrawal. However, withdrawal of consent may affect our ability to provide certain services or features.

3.2 Contractual Necessity

We process your personal information where necessary for the performance of a contract with you or to take steps at your request before entering into a contract, including:

(a) Creating and managing your account;

(b) Providing services requested by you;

(c) Processing transactions and payments;

(d) Fulfilling our obligations under our Terms of Service;

(e) Delivering customer support and assistance;

(f) Communicating with you about your account or transactions.

3.3 Legal Obligations

We process your personal information where necessary to comply with legal obligations to which we are subject, including:

(a) Compliance with financial regulations and anti-money laundering laws;

(b) Identity verification and Know Your Customer requirements;

(c) Tax reporting and withholding obligations;

(d) Responding to lawful requests from authorities;

(e) Maintaining records as required by law;

(f) Compliance with court orders and legal processes;

(g) Meeting data protection and privacy law requirements.

3.4 Legitimate Interests

We process your personal information where necessary for our legitimate interests or the legitimate interests of third parties, provided that such interests are not overridden by your fundamental rights and freedoms. Our legitimate interests include:

(a) **Business Operations:** Operating and managing our business efficiently, conducting business planning and administration, managing corporate transactions;

(b) **Platform Development:** Improving and developing our Platform, services, and features, conducting research and innovation, testing new technologies;

(c) **Security and Fraud Prevention:** Protecting the Platform and users from fraud, security threats, and illegal activities, ensuring platform security and integrity;

(d) **Marketing:** Promoting our Platform and services to relevant audiences, conducting market research, understanding customer needs and preferences;

(e) **Analytics:** Understanding how the Platform is used, analyzing trends and patterns, measuring performance and effectiveness;

(f) **Legal Protection:** Enforcing our legal rights, defending against legal claims, protecting our property and assets;

(g) **Customer Relationships:** Maintaining and developing relationships with customers, providing customer support, improving user experience.

3.5 Vital Interests

In rare circumstances, we may process your personal information where necessary to protect your vital interests or those of another person, such as in emergency situations involving life-threatening circumstances.

3.6 Public Interest

We may process your personal information where necessary for the performance of a task carried out in the public interest or in the exercise of official authority, if applicable.

---

4. INFORMATION SHARING AND DISCLOSURE

We may share, disclose, transfer, or otherwise make your personal information available to various third parties in the following circumstances:

4.1 Service Providers and Business Partners

We share information with third-party service providers, contractors, vendors, and business partners who perform services on our behalf or help us operate our business, including:

(a) **Technology and Infrastructure Providers:** Cloud hosting providers, server providers, content delivery networks, database services, backup and disaster recovery services, technical infrastructure providers;

(b) **Payment Processing and Financial Services:** Payment processors (Stripe, PayPal, etc.), payment gateways, merchant services providers, banking partners, cryptocurrency exchange services, fraud detection services, credit card processing companies;

(c) **Identity Verification and Compliance Services:** KYC/AML service providers, identity verification services, background check providers, sanctions screening services, document verification services, biometric verification providers;

(d) **Communication Services:** Email service providers, SMS/text messaging services, push notification services, customer communication platforms, call center services, live chat providers;

(e) **Analytics and Marketing Services:** Analytics platforms, marketing automation tools, advertising networks, social media platforms, survey and feedback tools, customer relationship management (CRM) systems, email marketing platforms;

(f) **Customer Support:** Customer support platforms, ticketing systems, helpdesk software, chat support tools, call recording services;

(g) **Security and Fraud Prevention:** Security services, fraud detection and prevention services, threat intelligence providers, vulnerability scanning services, penetration testing providers, cybersecurity firms;

(h) **Professional Services:** Legal counsel, accountants, auditors, consultants, advisors, business analysts, market research firms.

These service providers are contractually obligated to use your information only for the purposes of providing services to us and are required to maintain appropriate security measures. However, we are not responsible for the privacy practices of these third parties.

4.2 Corporate Affiliates and Related Entities

We may share information with our parent companies, subsidiaries, affiliates, related entities, and other companies under common ownership or control, for purposes including:

(a) Providing integrated services and features across multiple platforms;

(b) Consolidating data storage and management;

(c) Conducting centralized analytics and reporting;

(d) Managing business operations and administration;

(e) Sharing resources and infrastructure;

(f) Supporting corporate functions and shared services.

4.3 Business Transactions and Corporate Events

In connection with any actual or contemplated merger, acquisition, sale of assets, reorganization, financing, bankruptcy, insolvency, receivership, dissolution, or other corporate transaction or proceeding, we may:

(a) Disclose information to potential or actual purchasers, investors, acquirers, or their advisors;

(b) Transfer information as part of business assets;

(c) Share information during due diligence processes;

(d) Transfer information to successors or assigns;

(e) Provide information necessary to evaluate, negotiate, or complete transactions;

(f) Share information with legal, financial, and professional advisors involved in transactions.

Information shared in connection with such transactions will be subject to confidentiality obligations, though successors may use information in accordance with this Policy or as disclosed during the transaction.

4.4 Legal and Regulatory Authorities

We may disclose information to governmental authorities, regulatory bodies, law enforcement agencies, courts, and other public authorities when:

(a) Required by law, regulation, legal process, or governmental request;

(b) Responding to subpoenas, court orders, warrants, or other legal demands;

(c) Complying with legal obligations or regulatory requirements;

(d) Cooperating with law enforcement investigations;

(e) Responding to national security or public safety requests;

(f) Meeting tax reporting and withholding requirements;

(g) Complying with anti-money laundering and sanctions regulations;

(h) Reporting suspicious activities as required by law.

4.5 Protection of Rights and Safety

We may disclose information when we believe in good faith that disclosure is necessary to:

(a) Protect our rights, property, or safety, or the rights, property, or safety of users or third parties;

(b) Detect, prevent, or address fraud, security issues, or technical problems;

(c) Enforce our Terms of Service, policies, or agreements;

(d) Investigate violations of our terms or policies;

(e) Protect against legal liability or potential legal claims;

(f) Prevent harm to individuals or property;

(g) Defend against legal claims or litigation;

(h) Pursue available remedies or limit damages we may sustain.

4.6 With Your Consent

We may share information with third parties when you have provided explicit consent or direction to do so, including:

(a) When you authorize third-party services to access your information;

(b) When you direct us to share information with specific parties;

(c) When you participate in promotions or programs requiring information sharing;

(d) When you connect third-party applications or services to your account;

(e) When you post information publicly or in shared spaces.

4.7 Public and Community Features

If the Platform includes public or community features (such as forums, comments, reviews, social features, or user-generated content sections), information you post or share through these features may be:

(a) Publicly visible to other users and visitors;

(b) Searchable by search engines;

(c) Shared by other users;

(d) Used by us for promotional or marketing purposes;

(e) Retained even if you delete your account (in some cases).

You should exercise caution when posting information in public or shared areas.

4.8 Aggregated and De-identified Information

We may share aggregated, anonymized, or de-identified information that cannot reasonably be used to identify you with:

(a) Business partners and collaborators;

(b) Researchers and academic institutions;

(c) Industry associations and standards bodies;

(d) The public through reports, publications, or presentations;

(e) Media and press;

(f) Investors and stakeholders;

(g) Any other parties for any lawful purpose.

Such sharing does not constitute sharing of personal information as the data cannot identify individuals.

4.9 International Transfers

Given the global nature of our operations, we may transfer information to countries outside your country of residence, including countries that may not provide the same level of data protection. When we transfer information internationally:

(a) We implement appropriate safeguards such as standard contractual clauses, binding corporate rules, or other legally recognized transfer mechanisms;

(b) We ensure recipients provide adequate protection for your information;

(c) We comply with applicable data protection laws regarding international transfers;

(d) In some cases, transfers may be based on your consent or necessary for contractual performance.

By using the Platform, you acknowledge and consent to international transfers of your information.

---

5. DATA RETENTION

5.1 Retention Periods

We retain your personal information for as long as necessary to fulfill the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law. Retention periods vary depending on the type of information, the purposes for which it is used, and applicable legal requirements.

5.2 Factors Determining Retention

Factors we consider in determining retention periods include:

(a) **Legal and Regulatory Requirements:** Laws and regulations requiring retention of certain records for specific periods (e.g., financial records, transaction records, compliance records);

(b) **Contractual Obligations:** Retention requirements under contracts and agreements;

(c) **Legitimate Business Purposes:** Ongoing need for information to operate our business, provide services, resolve disputes, enforce agreements, or protect legal rights;

(d) **Statute of Limitations:** Periods during which legal claims may be brought;

(e) **User Account Status:** Whether your account is active or has been closed;

(f) **Type of Information:** Different categories of information may have different retention needs;

(g) **Technical Limitations:** Practical limitations on deletion from backup systems or archived records.

5.3 Specific Retention Examples

While retention periods vary, examples include:

(a) **Account Information:** Retained for the duration of your account relationship and for a reasonable period thereafter (typically 5-10 years) for legal, compliance, and business purposes;

(b) **Transaction and Financial Records:** Retained for periods required by financial regulations, tax laws, and anti-money laundering requirements (typically 5-10 years);

(c) **Communication Records:** Retained for periods necessary for business purposes, legal compliance, and dispute resolution (typically 3-7 years);

(d) **Marketing Information:** Retained until you unsubscribe or withdraw consent, and for reasonable periods thereafter for compliance and record-keeping;

(e) **Compliance and KYC Records:** Retained for periods required by regulations (typically 5-10 years after relationship ends);

(f) **Security and Fraud Investigation Records:** Retained for extended periods necessary to address security threats and prevent fraud;

(g) **Legal Records:** Retained for periods necessary to defend legal rights, during litigation, and for applicable statutes of limitations;

(h) **Technical Logs:** Typically retained for shorter periods (days to months) unless needed for security or legal purposes.

5.4 Deletion and Anonymization

After retention periods expire, we will:

(a) Securely delete or destroy personal information;

(b) Anonymize or de-identify information so it can no longer identify you;

(c) Aggregate information with other data;

(d) Archive information in secure, segregated systems with restricted access.

However, some information may be retained in backup systems or archives for longer periods due to technical limitations. We will take reasonable steps to ensure such retained information is not accessed or used except where required for legal or technical reasons.

5.5 Exceptions to Deletion

Even after retention periods or upon your request for deletion, we may retain information:

(a) To comply with legal or regulatory obligations;

(b) To resolve disputes or enforce agreements;

(c) To protect against fraud or security threats;

(d) For technical reasons (e.g., backup systems, cache);

(e) Where retention is necessary for our legitimate interests and not overridden by your rights;

(f) Where information has been anonymized or aggregated and no longer identifies you.

---

6. YOUR RIGHTS AND CHOICES

Depending on your location and applicable laws, you may have certain rights regarding your personal information:

6.1 Access and Information Rights

You may have the right to:

(a) **Access:** Request access to your personal information we hold and obtain a copy;

(b) **Information:** Request information about how we collect, use, and share your information;

(c) **Data Portability:** Receive your personal information in a structured, commonly used, machine-readable format and transmit it to another controller (where technically feasible).

6.2 Correction and Update Rights

You may have the right to:

(a) **Rectification:** Request correction of inaccurate or incomplete personal information;

(b) **Update:** Update your account information and preferences through your account settings.

6.3 Deletion and Erasure Rights

You may have the right to:

(a) **Erasure/Deletion:** Request deletion or removal of your personal information in certain circumstances;

(b) **Right to be Forgotten:** Request deletion of personal information when it is no longer necessary for the purposes collected, when consent is withdrawn, or when processing is unlawful.

However, deletion rights may be limited where we need to retain information for legal obligations, dispute resolution, fraud prevention, or other legitimate purposes.

6.4 Restriction and Objection Rights

You may have the right to:

(a) **Restriction of Processing:** Request restriction or limitation of processing your personal information in certain circumstances (e.g., while we verify accuracy, while assessing objections);

(b) **Object to Processing:** Object to processing based on legitimate interests or for direct marketing purposes;

(c) **Opt-Out:** Opt out of certain uses of your information, such as marketing communications.

6.5 Consent Withdrawal

Where processing is based on your consent, you have the right to:

(a) Withdraw consent at any time, without affecting the lawfulness of processing before withdrawal;

(b) Manage consent preferences through your account settings or by contacting us;

(c) Opt out of specific processing activities for which consent was given.

6.6 Automated Decision-Making Rights

If we engage in automated decision-making or profiling that produces legal or similarly significant effects, you may have the right to:

(a) Not be subject to decisions based solely on automated processing;

(b) Obtain human intervention in the decision-making process;

(c) Express your point of view and contest the decision;

(d) Obtain an explanation of the decision and the logic involved.

6.7 Communication Preferences

You can manage your communication preferences:

(a) **Marketing Emails:** Unsubscribe from marketing emails using the unsubscribe link in emails or through account settings;

(b) **Push Notifications:** Disable push notifications through device or application settings;

(c) **SMS/Text Messages:** Opt out by replying "STOP" or through account settings;

(d) **Communication Channels:** Choose preferred communication channels and frequency.

Note that even if you opt out of marketing communications, we may still send you transactional, administrative, or legally required communications.

6.8 Cookie and Tracking Preferences

You can manage cookies and tracking technologies through:

(a) **Browser Settings:** Configure browser settings to refuse cookies, delete cookies, or receive notifications when cookies are set;

(b) **Cookie Consent Tools:** Use any cookie consent management tools we provide on the Platform;

(c) **Opt-Out Links:** Use industry opt-out mechanisms for advertising cookies (e.g., Digital Advertising Alliance, Network Advertising Initiative);

(d) **Do Not Track:** Some browsers offer "Do Not Track" signals, though we may not respond to such signals given the lack of industry standards;

(e) **Mobile Settings:** Use mobile device settings to limit ad tracking or reset advertising identifiers.

Note that disabling cookies may affect platform functionality and your user experience.

6.9 Location Data Preferences

You can control location data collection through:

(a) **Device Settings:** Enable or disable location services for the Platform through device settings;

(b) **Application Permissions:** Manage location permissions through application settings;

(c) **Precision Settings:** Choose between precise and approximate location sharing where available.

6.10 Exercising Your Rights

To exercise your rights:

(a) **Contact Methods:** Submit requests through the contact information provided in Section 9 of this Policy;

(b) **Required Information:** Provide sufficient information to verify your identity and specify the right you wish to exercise;

(c) **Verification Process:** We may require verification of your identity before responding to requests to protect your privacy and security;

(d) **Response Time:** We will respond to requests within the timeframes required by applicable law (typically 30 days, with possible extensions where necessary);

(e) **No Fee:** We generally do not charge fees for responding to requests, except where requests are manifestly unfounded, excessive, or repetitive, in which case we may charge reasonable administrative costs or refuse the request.

6.11 Limitations and Exceptions

Your rights may be limited or unavailable in certain circumstances:

(a) Where responding would reveal confidential commercial information;

(b) Where responding would adversely affect others' rights and freedoms;

(c) Where we need to comply with legal obligations;

(d) Where retention is necessary for legal claims, fraud prevention, or security purposes;

(e) Where information has been anonymized or aggregated;

(f) Where technical limitations prevent compliance;

(g) As otherwise permitted or required by applicable law.

If we cannot fully comply with your request, we will explain the reasons and extent of our compliance.

6.12 Complaints and Supervisory Authorities

If you have concerns about our privacy practices or believe your rights have been violated:

(a) **Contact Us First:** We encourage you to contact us directly so we can address your concerns;

(b) **Supervisory Authorities:** Depending on your location, you may have the right to lodge a complaint with a data protection supervisory authority, such as:

- In the UK: Information Commissioner's Office (ICO)
- In the EU: Your local data protection authority
- In other jurisdictions: The relevant privacy or data protection regulator;

(c) **Legal Remedies:** You may also have the right to seek legal remedies through courts or other dispute resolution mechanisms.

---

7. DATA SECURITY AND PROTECTION

7.1 Security Measures

We implement reasonable administrative, technical, and physical security measures designed to protect your personal information from unauthorized access, use, disclosure, alteration, and destruction. These measures include:

Technical Safeguards: (a) Encryption of data in transit using SSL/TLS protocols; (b) Encryption of sensitive data at rest; (c) Secure authentication mechanisms and access controls; (d) Regular security updates and patches; (e) Firewalls, intrusion detection and prevention systems; (f) Vulnerability scanning and penetration testing; (g) Secure coding practices and code reviews; (h) Network segmentation and isolation of systems; (i) Regular security monitoring and logging.

Administrative Safeguards: (a) Access controls limiting who can access personal information based on role and need-to-know; (b) Background checks for employees with access to sensitive information; (c) Confidentiality agreements and obligations for employees and contractors; (d) Privacy and security training for personnel; (e) Incident response and breach notification procedures; (f) Regular security audits and assessments; (g) Third-party security assessments and certifications where appropriate; (h) Data protection impact assessments for high-risk processing.

Physical Safeguards: (a) Secure data center facilities with access controls; (b) Environmental controls and redundancy systems; (c) Secure disposal procedures for physical media; (d) Visitor management and monitoring systems; (e) Physical security measures at our offices and facilities.

7.2 Third-Party Security

We require third-party service providers with access to personal information to maintain appropriate security measures through contractual obligations. However, we cannot guarantee the security practices of third parties and are not responsible for their security measures.

7.3 Security Limitations and Disclaimer

IMPORTANT SECURITY DISCLAIMER:

Despite our security measures, you acknowledge and understand that:

(a) **No Absolute Security:** No system, platform, or method of data transmission or storage can be guaranteed to be absolutely secure, completely immune from breaches, or free from all vulnerabilities;

(b) **Inherent Internet Risks:** The internet and electronic communications are inherently insecure, and data transmitted over the internet may be intercepted, accessed, or compromised by unauthorized parties;

(c) **Evolving Threats:** Security threats constantly evolve, and new vulnerabilities and attack methods are continuously discovered;

(d) **User Responsibilities:** Security also depends on your actions, including maintaining confidentiality of credentials, using strong passwords, keeping devices secure, and being vigilant against phishing and social engineering;

(e) **Third-Party Risks:** We cannot control or guarantee the security of third-party systems, networks, or services you use to access the Platform.

7.4 Your Security Responsibilities

To help protect your information:

(a) Use strong, unique passwords and enable two-factor authentication where available; (b) Keep your login credentials confidential and do not share them; (c) Regularly update your passwords and security settings; (d) Keep your devices, browsers, and software up to date with security patches; (e) Be cautious of phishing attempts, suspicious emails, and social engineering; (f) Use secure networks and avoid public WiFi for sensitive activities; (g) Log out of your account when finished using shared or public devices; (h) Monitor your account activity and report suspicious activity immediately; (i) Review and adjust your privacy settings regularly.

7.5 Data Breach Notification

In the event of a security breach that affects your personal information:

(a) We will assess the breach and its impact on your privacy and security;

(b) We will take steps to contain and remediate the breach;

(c) Where required by applicable law, we will notify you and relevant authorities within the timeframes required by law;

(d) Notifications will include information about the nature of the breach, types of information affected, steps we are taking, and recommended actions you should take;

(e) We will cooperate with authorities in investigating and addressing breaches;

(f) We will implement measures to prevent similar incidents in the future.

7.6 Limitation of Liability for Security Incidents

CRITICAL NOTICE:

To the fullest extent permitted by law, we shall not be liable for any unauthorized access, security breaches, data breaches, cyber-attacks, hacking incidents, or other security incidents that result from circumstances beyond our reasonable control, including:

(a) Sophisticated attacks that circumvent standard security measures; (b) Zero-day vulnerabilities and advanced persistent threats; (c) Breaches of third-party systems or services; (d) Compromises resulting from your failure to maintain security of credentials; (e) Social engineering attacks targeting you or your organization; (f) Physical theft or loss of your devices; (g) Malware or viruses on your devices.

This limitation is in addition to the limitations of liability set forth in our Terms of Service.

---

8. CHILDREN'S PRIVACY

8.1 Age Restrictions

The Platform is not intended for, directed to, or designed to attract children under the age of 18 (or the age of majority in applicable jurisdictions). We do not knowingly collect, use, or disclose personal information from children under 18.

8.2 Parental Consent

If we learn that we have collected personal information from a child under 18 without proper parental consent (where required by law):

(a) We will take steps to delete such information as soon as reasonably possible;

(b) We may terminate or suspend the child's account;

(c) We will not use or disclose such information except as necessary to delete it or as required by law;

(d) Parents or legal guardians may contact us to request access to, correction of, or deletion of their child's information.

8.3 Parental Notification

If you are a parent or legal guardian and believe your child has provided personal information to us without your consent, please contact us immediately using the contact information in Section 9. Please provide sufficient information to enable us to identify and verify your child's information.

8.4 Special Protections

We take special precautions regarding children's privacy:

(a) We do not condition access to features or services on children providing more personal information than reasonably necessary;

(b) We take reasonable measures to ensure parental notice and consent where required;

(c) We provide parents with the ability to review and request deletion of their children's personal information;

(d) We maintain the confidentiality, security, and integrity of children's personal information;

(e) We limit retention of children's personal information to periods necessary for legitimate purposes or as required by law.

---

9. INTERNATIONAL DATA TRANSFERS

9.1 Global Operations

We operate globally and may transfer personal information to countries outside your country of residence, including to the United Kingdom, European Union, United States, and other countries where our service providers, partners, or data centers are located.

9.2 Different Data Protection Standards

Some countries may not provide the same level of data protection as your home country. Data protection laws and government surveillance practices vary significantly by country, and your information may be subject to access requests from governments, courts, or law enforcement in those countries according to their laws.

9.3 Transfer Safeguards

When we transfer personal information internationally, we implement appropriate safeguards, including:

(a) **Standard Contractual Clauses (SCCs):** Using European Commission-approved Standard Contractual Clauses or UK International Data Transfer Agreements for transfers from the EU/EEA or UK;

(b) **Adequacy Decisions:** Relying on adequacy decisions by the European Commission or UK authorities recognizing certain countries as providing adequate data protection;

(c) **Binding Corporate Rules:** Implementing binding corporate rules approved by data protection authorities;

(d) **Contractual Protections:** Requiring contractual commitments from recipients to protect transferred data;

(e) **Additional Measures:** Implementing supplementary technical, organizational, and contractual measures where appropriate;

(f) **Consent:** Obtaining your explicit consent for transfers where appropriate and legally required.

9.4 Transfers to the United States

Information may be transferred to and processed in the United States, which does not have an adequacy decision from the European Commission. When transferring to the US, we rely on appropriate safeguards such as Standard Contractual Clauses and, where applicable, additional measures to ensure adequate protection.

9.5 Acknowledgment and Consent

By using the Platform, you acknowledge and consent to:

(a) The transfer of your personal information to countries outside your country of residence;

(b) Processing of your information in countries with different data protection standards;

(c) The application of the laws of the countries where your information is processed, including laws governing access by government authorities;

(d) The risks associated with international transfers, including potential access by foreign governments.

9.6 Inquiries About Transfers

If you have questions about international transfers of your information, including the safeguards we use, please contact us using the information in Section 10.

---

10. COOKIES AND TRACKING TECHNOLOGIES

10.1 Types of Technologies Used

We and our service providers use various tracking technologies on the Platform, including:

Cookies: Small text files stored on your device that contain information about your browsing activity and preferences. Cookies may be:

- **Session Cookies:** Temporary cookies that expire when you close your browser;
- **Persistent Cookies:** Cookies that remain on your device for a set period or until deleted;
- **First-Party Cookies:** Set by us directly;
- **Third-Party Cookies:** Set by our service providers or partners.

Web Beacons/Pixels: Small graphic images embedded in web pages, emails, or applications that track whether content has been viewed, when it was viewed, and from which IP address.

Scripts: Code embedded in web pages that enables certain functionality and collects information about your interaction with the Platform.

Local Storage: Technologies like HTML5 local storage that allow storage of data locally on your device.

SDKs and APIs: Software development kits and application programming interfaces integrated into mobile applications that collect usage and device information.

Fingerprinting Technologies: Technologies that collect information about your device configuration to create a unique identifier.

10.2 Purposes of Tracking Technologies

We use these technologies for various purposes:

Essential/Functional Purposes: (a) Authentication and security; (b) Remembering your preferences and settings; (c) Enabling platform features and functionality; (d) Load balancing and platform optimization; (e) Fraud prevention and security monitoring.

Analytics and Performance: (a) Understanding how the Platform is used; (b) Analyzing traffic, usage patterns, and trends; (c) Measuring feature performance and effectiveness; (d) Identifying technical issues and errors; (e) Conducting A/B testing and experimentation; (f) Generating reports and insights.

Personalization: (a) Remembering your preferences and customizing content; (b) Providing personalized recommendations; (c) Tailoring your user experience; (d) Showing relevant content and features.

Advertising and Marketing: (a) Delivering targeted advertising based on your interests; (b) Measuring advertising effectiveness and campaign performance; (c) Frequency capping and ad delivery optimization; (d) Retargeting and remarketing

to users who visited the Platform; (e) Attribution and conversion tracking; (f) Building advertising audiences and profiles.

10.3 Third-Party Cookies and Technologies

Third parties may set cookies and use tracking technologies on the Platform, including:

(a) **Analytics Providers:** Google Analytics, Mixpanel, Amplitude, and similar services that help us understand platform usage;

(b) **Advertising Networks:** Ad networks and exchanges that deliver targeted advertising and measure ad performance;

(c) **Social Media Platforms:** Social media plugins and widgets (like Facebook, Twitter, LinkedIn) that enable social features and track your interactions;

(d) **Marketing Technology:** Marketing automation platforms, tag management systems, and optimization tools;

(e) **Customer Support:** Live chat, helpdesk, and customer support tools;

(f) **Security Services:** Fraud prevention, bot detection, and security services.

These third parties may collect information about your online activities over time and across different websites and services. We do not control these third parties' tracking technologies or data practices. Please review their privacy policies for information about their practices.

10.4 Managing Cookie Preferences

You can control cookies and tracking technologies through:

Browser Controls: Most browsers allow you to:

- View, manage, and delete cookies;
- Block all cookies or third-party cookies;
- Receive notifications when cookies are set;
- Clear cookies when closing the browser.

Access these controls through your browser settings or help menu. Note that different browsers have different procedures.

Opt-Out Tools: For advertising cookies, you can opt out through:

- Digital Advertising Alliance (DAA): www.aboutads.info/choices
- Network Advertising Initiative (NAI): www.networkadvertising.org/choices

- European Interactive Digital Advertising Alliance (EDAA): www.youronlinechoices.eu
- Google Ads Settings: www.google.com/settings/ads

Mobile Device Settings: On mobile devices, you can:

- Limit ad tracking through device privacy settings;
- Reset your advertising identifier;
- Manage app permissions and data access;
- Control location services.

Do Not Track: Some browsers offer "Do Not Track" (DNT) signals. Currently, there is no industry standard for responding to DNT signals, and we may not respond to such signals. We will update this Policy if standards emerge and we adopt them.

10.5 Consequences of Disabling Cookies

If you disable or refuse cookies:

(a) Some features and functionality may not work properly; (b) You may not be able to access certain areas of the Platform; (c) Your preferences and settings may not be saved; (d) You may see less relevant advertising; (e) We may not be able to provide personalized experiences; (f) Platform performance may be affected.

Essential cookies necessary for platform functionality may still be used even if you disable other cookies.

---

11. CHANGES TO THIS PRIVACY POLICY

11.1 Right to Modify

We reserve the right to modify, update, amend, or change this Privacy Policy at any time, in our sole discretion, for any reason or no reason. We may make changes to:

(a) Reflect changes in our information practices; (b) Accommodate new technologies or services; (c) Comply with legal or regulatory requirements; (d) Improve clarity or readability; (e) Address user feedback or concerns; (f) Align with business changes or strategies; (g) For any other reason we deem appropriate.

11.2 Notification of Changes

When we make changes to this Privacy Policy:

(a) We will update the "Last Updated" date at the top of this Policy;

(b) We will post the revised Policy on the Platform;

(c) For material changes that significantly affect your rights or our practices, we may provide additional notice through:

- Email notification to the address associated with your account;
- Prominent notice or banner on the Platform;
- In-app notifications or alerts;
- Other reasonable means of communication;

(d) However, we are not obligated to provide enhanced notice, and posting the revised Policy on the Platform may be our only notice method.

11.3 Effective Date and Acceptance

Changes to this Privacy Policy become effective:

(a) Immediately upon posting to the Platform, unless we specify a later effective date;

(b) At such other date as we may specify in the revised Policy.

Your continued use of the Platform after changes become effective constitutes your acceptance of the revised Privacy Policy. If you do not agree to changes, you must stop using the Platform.

11.4 Responsibility to Review

It is your responsibility to regularly review this Privacy Policy to stay informed of changes. We encourage you to check the "Last Updated" date and review this Policy periodically. Your use of the Platform following changes indicates your acknowledgment and acceptance of the revised terms.

11.5 Material Changes

For material changes that substantively expand our rights to use your personal information, we may seek your consent where required by applicable law before applying changes to information collected before the change.

---

12. ADDITIONAL JURISDICTION-SPECIFIC PROVISIONS

12.1 European Economic Area (EEA), United Kingdom, and Switzerland

If you are located in the EEA, UK, or Switzerland, additional protections apply:

Legal Basis: We process your data based on the legal grounds described in Section 3, including consent, contractual necessity, legal obligations, and legitimate interests.

Data Controller: PAYMENT ASSIST LTD is the data controller responsible for your personal data.

Your Rights: You have the rights described in Section 6, including rights of access, rectification, erasure, restriction, data portability, and objection. You also have the right to lodge a complaint with your local supervisory authority.

Transfers: We transfer data outside the EEA/UK using appropriate safeguards such as Standard Contractual Clauses.

Retention: We retain data only for as long as necessary for the purposes described in this Policy or as required by law.

Profiling: If we engage in profiling or automated decision-making with legal or significant effects, you have rights to human intervention and explanation.

12.2 California Residents

If you are a California resident, the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) provide additional rights:

Right to Know: You can request information about: categories of personal information collected; categories of sources; business or commercial purposes for collection; categories of third parties with whom we share information; and specific pieces of information we've collected.

Right to Delete: You can request deletion of personal information we collected from you, subject to certain exceptions.

Right to Correct: You can request correction of inaccurate personal information.

Right to Opt-Out: You can opt out of the "sale" or "sharing" of personal information (as those terms are defined under California law). Note: Given the demonstrative nature of our Platform and our practices, we do not believe we "sell" personal information in the traditional sense, though some data sharing practices might be construed as "sales" under California's broad definition.

Right to Limit Use of Sensitive Personal Information: You can limit our use of sensitive personal information to purposes necessary for providing services.

Right to Non-Discrimination: We will not discriminate against you for exercising your privacy rights.

Shine the Light: California Civil Code Section 1798.83 permits you to request information about disclosure of personal information to third parties for their direct

marketing purposes. We do not currently share personal information with third parties for their direct marketing purposes.

Do Not Track: We do not currently respond to "Do Not Track" signals.

Authorized Agents: You may designate an authorized agent to make requests on your behalf. We may require verification of the agent's authority.

Contact for Requests: To exercise these rights, contact us using the information in Section 13.

12.3 Nevada Residents

Nevada residents have the right to opt out of the "sale" of certain covered information. We do not believe we sell covered information as defined under Nevada law. If you are a Nevada resident and wish to exercise this right, contact us at the information in Section 13.

12.4 Other Jurisdictions

If you reside in other jurisdictions with specific privacy laws (such as Brazil's LGPD, Canada's PIPEDA, Australia's Privacy Act, etc.), you may have additional rights under those laws. Please contact us to inquire about rights specific to your jurisdiction.

---

13. CONTACT INFORMATION

13.1 Privacy Inquiries and Requests

For questions, concerns, or requests regarding this Privacy Policy or our privacy practices, or to exercise your privacy rights, please contact us:

Email: [You would typically include an email address, but given the demonstrative nature of the platform, you may choose to include or omit this]

Mailing Address:
Privacy Department
PAYMENT ASSIST LTD
Pera Business Park
Nottingham Road
Melton Mowbray
Leicestershire, England
LE13 0PB
United Kingdom

Company Registration Number: 08752986

13.2 Data Protection Officer

If required by applicable law, we will appoint a Data Protection Officer (DPO). If you wish to contact our DPO (if appointed), use the contact information above and mark your communication "Attention: Data Protection Officer."

13.3 Supervisory Authority Contact

If you are located in the EEA or UK and believe we have not adequately addressed your concerns, you may contact your local supervisory authority:

For UK Residents:
Information Commissioner's Office (ICO)
Website: www.ico.org.uk
Telephone: 0303 123 1113

For EEA Residents:
Contact your local data protection authority. A list is available at: https://edpb.europa.eu/about-edpb/board/members_en

13.4 Response to Inquiries

We will make reasonable efforts to respond to inquiries and requests within timeframes required by applicable law. We may require verification of your identity before responding to requests involving personal information. Please provide sufficient information to enable us to identify you and verify your request.

---

14. ADDITIONAL IMPORTANT INFORMATION

14.1 Platform Demonstration Nature

IMPORTANT REMINDER:

As described in our Terms of Service, the Snap Wallet Platform is primarily a demonstration and informational service. This Privacy Policy describes our information practices comprehensively, but you should be aware that:

(a) The extent to which various features and services are operational may be limited;

(b) Information collection and use is subject to the availability and functionality of Platform features;

(c) This Policy describes practices that may apply if and when features are implemented and operational;

(d) Our information practices may evolve as the Platform develops.

14.2 Links to Third-Party Websites and Services

The Platform may contain links to third-party websites, services, applications, or resources that are not owned, controlled, or operated by us. This Privacy Policy does not apply to such third parties. We are not responsible for the privacy practices, content, or security of third-party sites and services.

We encourage you to review the privacy policies and terms of service of any third-party sites or services before providing them with personal information or engaging with them. Your use of third-party sites and services is at your own risk.

14.3 Social Media and Public Forums

If the Platform includes social features, forums, comments sections, or other public areas where users can post content:

(a) Information you post may be visible to other users and the public;

(b) Other users may use, copy, or share your posted information;

(c) We may use your posts for promotional or other purposes;

(d) Posted information may be indexed by search engines and appear in search results;

(e) Even if you delete your account, your posts may remain visible or accessible;

(f) We may moderate, edit, or remove posts at our discretion.

Exercise caution when posting personal information in public areas.

14.4 Employment Applications

If you apply for employment with us through the Platform or otherwise:

(a) We will collect information you provide in your application, resume, cover letter, and related materials;

(b) We may collect additional information during the recruitment process (references, background checks, assessments);

(c) We will use this information to evaluate your application, conduct the recruitment process, and comply with employment laws;

(d) We will retain application materials as required by law and for legitimate business purposes;

(e) Employment applicant data may be subject to different retention periods and practices than general user data.

14.5 Aggregated and Anonymized Data

We may create aggregated, anonymized, or de-identified data from personal information by removing information that makes the data personally identifiable.

We may use, share, and disclose such data for any purpose without restriction, as it does not identify individuals. This data is not subject to this Privacy Policy once properly anonymized.

14.6 Business Analytics and Research

We may use personal information for business analytics, research, and insights to:

(a) Understand market trends and customer needs;

(b) Develop new products, services, and features;

(c) Improve existing offerings and operations;

(d) Create reports, case studies, and thought leadership content (with appropriate anonymization);

(e) Support strategic decision-making;

(f) Benchmark performance against industry standards.

14.7 Compliance with Laws

We may collect, use, disclose, and retain personal information as necessary to comply with applicable laws, regulations, legal processes, and governmental requests, including:

(a) Financial regulations and reporting requirements;

(b) Anti-money laundering and sanctions laws;

(c) Tax laws and reporting obligations;

(d) Consumer protection laws;

(e) Data protection and privacy laws;

(f) Employment laws;

(g) Intellectual property laws;

(h) Any other applicable legal requirements.

---

15. ACCEPTANCE OF THIS PRIVACY POLICY

IMPORTANT NOTICE:

BY ACCESSING, BROWSING, USING, OR INTERACTING WITH THE SNAP WALLET PLATFORM IN ANY MANNER, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD, AND AGREE TO BE BOUND BY THIS PRIVACY POLICY IN ITS ENTIRETY.

YOUR USE OF THE PLATFORM CONSTITUTES YOUR ACCEPTANCE OF THIS PRIVACY POLICY AND YOUR CONSENT TO THE COLLECTION, USE, PROCESSING, STORAGE, SHARING, AND DISCLOSURE OF YOUR PERSONAL INFORMATION AS DESCRIBED HEREIN.

IF YOU DO NOT AGREE TO THIS PRIVACY POLICY, YOU MUST NOT ACCESS OR USE THE PLATFORM.

Your continued use of the Platform following any changes to this Privacy Policy constitutes your acceptance of such changes.