1. Introduction and Scope

1.1 **Purpose of this Policy**
This Privacy Policy ("Policy") explains how Anytime Technologies Limited, trading as **PAY247** ("PAY247," "we," "our," or "us"), collects, uses, shares, and protects Personal Data in connection with our payment gateway, payout, and related technology services ("Services").

1.2 **Scope**
This Policy applies to Personal Data processed by PAY247 in the following contexts:
(a) **Merchants and business users** who register for, integrate, or use PAY247 Services;
(b) **End Users or payers** whose transactions are processed through PAY247 on behalf of Merchants;
(c) **Visitors** to PAY247's websites, dashboards, or APIs; and
(d) **Partners, suppliers, and applicants** who engage with PAY247 for business purposes.

1.3 **Commercial Nature of Services**
PAY247's Services are provided for **business and professional use**. We do not offer consumer accounts or wallet products directly to individuals. End users who make payments through a Merchant integrated with PAY247 should direct service inquiries or rights requests primarily to the relevant Merchant.

1.4 **Relationship with Other Documents**
This Policy supplements, and forms part of, the PAY247 Terms and Conditions, KYC & AML Policy, and Cookie Policy. In case of conflict, this Policy governs data-protection matters.

1.5 **Territorial Scope**
PAY247 is established in the British Virgin Islands ("BVI") and processes data globally through partner institutions and infrastructure in multiple regions. We comply with the BVI Data Protection Act (2021) and applicable international privacy laws where we operate or where our users are located.

2. Definitions

For purposes of this Policy, the following definitions apply:

- **"Personal Data"** (or **"Personal Information"**) means any information that identifies, relates to, or can reasonably be associated with an individual.
- **"Processing"** means any operation performed on Personal Data, such as collection, use, disclosure, storage, transmission, or deletion.
- **"Controller"** means the entity that determines the purposes and means of Processing.
- **"Processor"** means the entity that processes Personal Data on behalf of a Controller.
- **"End User"** or **"Payer"** means an individual who initiates or receives a payment through a Merchant using PAY247.
- **"Merchant"** means a business entity using PAY247's platform to receive or send payments.

- **“Sensitive Personal Data”** means data relating to government IDs, financial accounts, biometrics, or other categories requiring higher protection under applicable law.
- **“Applicable Law”** means data-protection and privacy laws in force where the data subject resides or where PAY247 operates, including the BVI Data Protection Act (2021), EU/UK GDPR, the California Consumer Privacy Act as amended by the CPRA, Brazil’s LGPD, Singapore’s PDPA, India’s Digital Personal Data Protection Act (2023), and China’s PIPL.

Terms not defined herein shall have the meanings given in those laws.

3. Who We Are and How to Contact Us

3.1 **Entity Responsible for Processing**
The entity responsible for data processing under this Policy is:

Anytime Technologies Limited (trading as PAY247)
Asia Leading Chambers, Road Town, Tortola, VG1110, British Virgin Islands.

3.2 **Privacy Contact**
For privacy-related inquiries, access requests, or complaints, you may contact us at:

privacy@pay247.io

3.3 **EU and UK Representatives**
If required by Article 27 of the EU/UK GDPR, PAY247 may appoint an authorised representative within the European Union and the United Kingdom. Representative details, once appointed, will be published at https://www.pay247.io/legal/privacy.

3.4 **Data Protection Officer (Optional)**
Where a Data Protection Officer (“DPO”) is designated, their contact information will be available through the same channel. PAY247 is not presently required by law to appoint a DPO but monitors its processing activities and will appoint one if thresholds are triggered.

4. Role Allocation: Controller and Processor

4.1 **Processor for Merchant Transactions**
PAY247 acts as a **data processor (service provider)** when processing End User payment data on behalf of a Merchant. In this capacity, PAY247 processes information solely under the Merchant’s instructions and in accordance with contractual obligations and applicable data-processing addenda.

4.2 **Independent Controller for Compliance and Risk**
PAY247 acts as an **independent data controller** when processing Personal Data for its own legitimate business and legal purposes, including:
(a) compliance with AML/CFT and sanctions obligations;
(b) fraud detection, transaction monitoring, and risk analysis;
(c) maintaining network and information security;

(d) conducting analytics and service improvement not involving profiling for marketing; and
(e) fulfilling statutory recordkeeping or reporting duties.

4.3 **Joint Controllers**
In limited instances, PAY247 may act as a joint controller with a Partner Institution (for example, an acquiring bank jointly determining transaction-monitoring parameters). In such cases, each entity remains responsible for its respective legal obligations.

4.4 **Third-Party Processors**
When PAY247 engages service providers to process data on its behalf (cloud hosting, analytics, KYC verification), those processors act under written contracts ensuring equivalent confidentiality, security, and data-protection standards.

4.5 **Responsibility Matrix**
Merchants remain responsible for providing End Users with appropriate privacy notices, obtaining necessary consents, and ensuring lawful collection of End User data transmitted through PAY247.

5. Categories of Personal Data We Process

PAY247 limits data collection to what is necessary for lawful and efficient operation of its Services. The types of Personal Data we may process include:

(a) **Merchant and Business Account Data** — company name, registration number, directors and shareholders, beneficial owners, authorised signatories, contact names, email addresses, phone numbers, business addresses, settlement bank details, and related documents.

(b) **End-User / Payer Data (processed for Merchants)** — name, email, billing information, transaction amount, date/time, masked card data or token, bank details, and transaction identifiers. PAY247 does not store raw cardholder data; this is handled by licensed acquirers.

(c) **KYC and Compliance Data** — identity documents, proof of address, company registration certificates, beneficial ownership information, sanctions and PEP screening results, and related compliance notes.

(d) **Technical and Device Data** — IP address, browser type, operating system, device identifiers, session logs, usage timestamps, and network information generated by interactions with PAY247 systems.

(e) **Communication Data** — correspondence, support tickets, call recordings, or emails exchanged with PAY247 staff.

(f) **Website and Cookie Data** — browsing metrics, session cookies, analytics identifiers, and user preferences (as described in the Cookie Policy).

(g) **Recruitment and Vendor Data** — CVs, professional history, tax identifiers, and banking details of suppliers or job applicants, where applicable.

6. Sources of Personal Data

We obtain Personal Data from several lawful and transparent sources:

(a) **Directly from you** — when you create an account, submit KYC documentation, or communicate with us.
(b) **From your organisation or Merchant** — where your employer or service provider registers you as an authorised user.
(c) **From Partner Institutions** — such as acquirers, banks, or payment processors who route or settle transactions through our platform.
(d) **From third-party verification or risk vendors** — including sanctions lists, PEP databases, fraud-detection engines, and identity-verification services.
(e) **From public or government sources** — corporate registries, regulatory filings, or public watchlists.
(f) **Automatically through your device or browser** — via cookies, logs, and similar technologies (see Section 10).

PAY247 does not knowingly purchase personal data from brokers or data sellers.

7. Purposes of Processing

We process Personal Data only where necessary for defined, legitimate, and proportionate purposes, namely:

(a) **Service Provision and Account Management**
To operate and maintain our payment gateway, APIs, dashboards, and support functions; to authenticate users; and to manage Merchant accounts and settlements.

(b) **Payment Processing and Transaction Execution**
To route, authorise, and reconcile payments between Merchants, End Users, and Partner Institutions; and to transmit relevant transaction details to complete lawful payments.

(c) **Risk Management and Fraud Prevention**
To detect and prevent fraudulent, suspicious, or prohibited transactions; to perform risk scoring and velocity checks; and to ensure the integrity of PAY247's systems.

(d) **KYC, AML, and Sanctions Compliance**
To identify and verify customers, monitor transactions, and fulfil legal obligations under the BVI Anti-Money Laundering Regulations (2008), FATF Recommendations, and analogous global standards.

(e) **Legal and Regulatory Obligations**
To maintain records, file reports, and respond to lawful requests from regulators, tax authorities, or law enforcement agencies.

(f) **Security and System Integrity**
To protect PAY247's infrastructure, prevent cyber threats, ensure network resilience, and conduct audits and troubleshooting.

(g) **Service Improvement and Analytics**
To analyse aggregated and pseudonymised usage data for improving functionality, performance, and user experience. Analytics are performed without building marketing profiles.

(h) **Communications**
To send operational or administrative messages, updates on changes to policies or system maintenance, and limited non-promotional notices relevant to merchants' existing services.

(i) **Corporate and Administrative Functions**
To manage vendors, suppliers, job applicants, and internal governance processes, including due diligence and recruitment.

8. Legal Bases for Processing

8.1 **General Principle**
PAY247 processes Personal Data only where there is a lawful basis under Applicable Law. Different bases may apply depending on the jurisdiction and the specific purpose.

8.2 **Contractual Necessity**
Processing necessary to perform our agreement with you or your organisation, such as:

- providing payment and payout services;
- verifying identity, enabling transactions, and communicating service updates.

8.3 **Legal Obligation**
Processing required to comply with laws and regulations, including:

- anti–money laundering, counter-terrorist financing, and sanctions screening;
- tax and accounting requirements;
- statutory reporting to regulators and law enforcement.

8.4 **Legitimate Interests**
Processing necessary for our legitimate interests, provided these are not overridden by the individual's rights, such as:

- ensuring network and information security;
- preventing fraud and abuse;
- improving and developing our Services;

- managing relationships with merchants and partners.

8.5 **Consent**
Where required by law (e.g., for non-essential cookies or marketing communications), we will seek consent. Consent may be withdrawn at any time without affecting prior lawful processing.

8.6 **Vital or Public Interest**
In rare cases, PAY247 may process data to protect vital interests (e.g., prevent fraud or harm) or to comply with requests from public authorities where disclosure is legally mandated.

9. No Sale or Cross-Context Behavioral Advertising

9.1 **No Sale of Personal Data**
PAY247 does **not sell** Personal Data as defined under the California Consumer Privacy Act (CCPA/CPRA) or equivalent global laws.

9.2 **No Cross-Context Behavioral Advertising**
PAY247 does **not share** Personal Data for cross-context behavioral advertising or tracking across non-affiliated websites or applications.

9.3 **Future Activities**
If PAY247 introduces new processing that qualifies as "sale" or "sharing" under applicable law, we will update this Policy and provide applicable opt-out rights before such activity occurs.

10. Cookies and Similar Technologies

10.1 **Use of Cookies**
Our websites and dashboards use cookies and similar technologies to operate securely, remember preferences, and analyse aggregated traffic.

10.2 **Categories of Cookies**
(a) *Strictly Necessary Cookies* – essential for login, session continuity, and fraud prevention; cannot be disabled.
(b) *Functional Cookies* – enhance user experience by storing preferences.
(c) *Analytics Cookies* – collect aggregated statistics to improve service performance.
(d) *Advertising Cookies* – rarely used; disabled by default in EEA/UK unless explicit consent is obtained.

10.3 **Consent Requirements**
PAY247 seeks prior consent where required by the EU ePrivacy Directive, UK PECR, or similar frameworks. In other jurisdictions, you may disable cookies via browser settings.

10.4 **Third-Party Analytics**
We use privacy-respecting analytics providers that process data in pseudonymised form; we do not allow them to use data for their own marketing.

10.5 **Do-Not-Track and Global Privacy Controls**
PAY247 honours valid Global Privacy Control (GPC) signals in jurisdictions recognising them (e.g., California, Colorado).

10.6 **More Information**
Details on specific cookies, durations, and configuration options are available in our **Cookie Policy** at https://www.pay247.io/legal/cookies.

11. Automated Decision-Making and Profiling

11.1 **Automated Fraud and Risk Screening**
PAY247 uses automated systems to identify potentially fraudulent transactions, unusual patterns, or policy violations.

11.2 **Human Oversight**
All automated decisions with legal or significant effects (e.g., transaction blocking or account suspension) are subject to human review by compliance analysts before final action.

11.3 **Rights in Automated Decisions**
Individuals in the EEA/UK and certain other jurisdictions may request:

- information about logic involved in automated processing;
- human intervention; or
- to contest decisions affecting them.
  Requests may be made through the contact details in Section 3.

11.4 **No Automated Marketing Profiles**
PAY247 does not build behavioural or marketing profiles based on user activity.

12. Data Sharing and Disclosure

12.1 **Principle of Limited Disclosure**
We share Personal Data only where necessary, lawful, and consistent with this Policy.

12.2 **Categories of Recipients**
(a) *Partner Institutions* – acquiring banks, payout partners, and regulated payment service providers for transaction settlement.
(b) *KYC/AML Vendors* – identity-verification, sanctions-screening, and fraud-detection providers.
(c) *Service Providers* – cloud infrastructure, hosting, analytics, customer support, and communications tools under written contracts.
(d) *Professional Advisors* – lawyers, auditors, and consultants under confidentiality obligations.
(e) *Authorities and Regulators* – law enforcement, tax, financial intelligence units, or courts when legally required.
(f) *Corporate Affiliates or Successors* – within PAY247's group or in connection with a merger or restructuring, subject to this Policy's safeguards.

12.3 **Independent Controllers**
Some third parties (e.g., card networks, issuing banks) act as independent controllers for their own compliance and dispute purposes. Their privacy notices govern their use of data.

12.4 **Prohibition on Unauthorised Disclosure**
PAY247 does not permit unauthorised onward disclosure or use of Personal Data by its processors for independent purposes.

13. International Data Transfers

13.1 **Global Operations**
Because PAY247 operates globally, Personal Data may be transferred to and processed in countries outside the BVI and the country of origin.

13.2 **Transfer Safeguards**
When transferring data internationally, PAY247 implements lawful mechanisms such as:

- **Standard Contractual Clauses (SCCs)** adopted by the European Commission;
- **UK International Data Transfer Addendum (IDTA)**;
- **BCR-equivalent contractual safeguards** with partners; and
- **Encryption and access-limitation controls** to protect data in transit and at rest.

13.3 **Data-Localization Laws**
Where local law requires (e.g., under China's PIPL or India's DPDP), PAY247 ensures local storage or approved transfer assessments before cross-border movement.

13.4 **Access by Authorities**
We review government requests and disclose data only where legally compelled, minimising scope to what is strictly required.

13.5 **Further Information**
Copies of applicable safeguards (redacted where necessary) may be requested by contacting privacy@pay247.io.

14. Data Retention

14.1 **Retention Principle**
Personal Data is retained only for as long as necessary to fulfil the purposes described in this Policy or to meet legal, regulatory, or partner obligations.

14.2 **Operational Retention Periods**
(a) Merchant and account data – retained during the contractual relationship and for at least **five (5) years** thereafter in line with BVI AML obligations.
(b) Transaction data – retained for statutory audit and regulatory purposes for **five (5) to seven (7) years**, depending on jurisdiction.
(c) Log and analytics data – typically retained for **up to 24 months** unless required for security

or troubleshooting.
(d) Support correspondence – retained for **up to three (3) years**.
(e) Recruitment data – retained for **one (1) year** unless employment is offered.

14.3 **Legal Hold**
If PAY247 is involved in a dispute or investigation, relevant records may be retained until resolution, even if retention exceeds normal periods.

14.4 **Deletion and Anonymisation**
Upon expiry of retention periods, data will be securely deleted or anonymised such that it can no longer identify individuals.

14.5 **Merchant Obligations**
Merchants remain responsible for retaining or deleting End-User data in accordance with their own legal obligations and privacy notices.

15. Data Security

15.1 **Security Commitment**
PAY247 maintains administrative, technical, and physical safeguards designed to protect Personal Data from unauthorised access, use, alteration, or destruction.

15.2 **Security Measures**
Safeguards include:

- encryption in transit (TLS 1.2 or higher) and at rest;
- strict access controls and multi-factor authentication for privileged systems;
- segregation of environments for production, test, and compliance data;
- continuous monitoring, intrusion detection, and vulnerability management; and
- employee background screening and confidentiality undertakings.

15.3 **Incident Response**
PAY247 maintains an incident-response plan. In the event of a confirmed data incident, PAY247 will:
(a) contain and assess the breach;
(b) notify affected Merchants and, where required, competent authorities within statutory timelines; and
(c) cooperate in remediation and mitigation efforts.

15.4 **Merchant Responsibilities**
Merchants must implement appropriate security measures within their own systems and promptly notify PAY247 of any compromise affecting credentials, API keys, or End-User data shared via the Services.

15.5 **Disclaimer**
While PAY247 uses commercially reasonable security measures, no online system can be fully immune from intrusion; therefore, PAY247 cannot guarantee absolute security.

16. Individual Privacy Rights

16.1 **General Rights**
Subject to Applicable Law, individuals may exercise the following rights:

- **Access:** to obtain confirmation whether we hold their Personal Data.
- **Correction:** to rectify inaccurate or incomplete information.
- **Deletion/Erasure:** to request deletion where data is no longer needed or unlawfully processed.
- **Restriction:** to limit processing in certain circumstances.
- **Portability:** to receive a copy of provided data in machine-readable format.
- **Objection:** to object to processing based on legitimate interests or to direct marketing.
- **Withdraw Consent:** to withdraw consent where processing is based on it.

16.2 **How to Exercise**
Requests may be made by email to **privacy@pay247.io**. PAY247 may require verification of identity before fulfilling any request.

16.3 **Response Timeframes**
PAY247 aims to respond within **one month** of receipt (or as permitted by local law). Complex or high-volume requests may take longer, in which case we will inform the requester.

16.4 **Denials and Appeals**
If PAY247 declines a request, reasons will be provided. Individuals may lodge a complaint with their local data-protection authority or the BVI Office of the Information Commissioner.

16.5 **No Discrimination**
PAY247 will not deny services or charge different rates because an individual exercised a privacy right.

17. Regional and Jurisdiction-Specific Disclosures

17.1 **European Economic Area (EEA) and United Kingdom**

- Data subjects have rights under Articles 15–22 GDPR.
- Transfers rely on Standard Contractual Clauses or other lawful mechanisms.
- Complaints may be raised with local supervisory authorities or the UK ICO.

17.2 **California, Colorado, and Other U.S. States**

- Residents may exercise rights to know, correct, and delete Personal Information.

- PAY247 does not sell or share Personal Information or use it for cross-context behavioral advertising.
- Global Privacy Control signals are honoured.

17.3 **Brazil (LGPD)**

- Processing bases include contract performance, legal obligation, and legitimate interest.
- Data subjects may contact PAY247 for rights under Articles 18–20 LGPD.
- Enquiries may also be directed to the **ANPD** (Autoridade Nacional de Proteção de Dados).

17.4 **Singapore (PDPA)**

- PAY247 relies on deemed consent for business communications and explicit consent where required.
- Individuals may request access and correction under Sections 21 and 22 PDPA.

17.5 **India (DPDP Act 2023)**

- PAY247 acts as a "Data Fiduciary." Individuals may request correction or erasure and raise grievances through **privacy@pay247.io**.

17.6 **People's Republic of China (PIPL)**

- Separate consent is obtained where required for cross-border transfers.
- PAY247 stores and transfers data in compliance with PIPL requirements and security assessments where applicable.

17.7 **British Virgin Islands (BVI)**

- PAY247 complies with the **Data Protection Act 2021**, which sets principles of fairness, purpose limitation, accuracy, and security.
- Individuals may contact the **Office of the Information Commissioner** for redress.

18. KYC, AML, and Sanctions Processing

18.1 **Legal Obligation Basis**
Processing for KYC, AML, and sanctions purposes is carried out under statutory obligations arising from BVI AML Regulations 2008, the Anti-Money Laundering and Terrorist Financing Code 2008, and corresponding global standards.

18.2 **Scope of Data**
Includes identification, verification, beneficial ownership, sanctions screening, and transaction monitoring information.

18.3 **Disclosure to Authorities**
Data may be shared with the **Financial Investigation Agency (FIA)**, Financial Services Commission, and other competent authorities where legally required.

18.4 **Retention Override**
AML/KYC data must be retained for a minimum of **five (5) years** after the relationship ends, overriding any deletion request.

18.5 **No Tipping-Off**
PAY247 employees and Merchants are prohibited from informing any person who is the subject of a suspicious activity report.

19. Children's Data

19.1 **Not Directed to Children**
PAY247 Services and websites are intended for adults engaged in commercial activities. They are **not directed to children under 16** years of age (or the age defined by local law).

19.2 **No Knowing Collection**
We do not knowingly collect or process children's Personal Data. Merchants must not submit minors' data to PAY247 unless permitted by applicable law and parental consent is obtained.

19.3 **Remedial Actions**
If PAY247 becomes aware that it has inadvertently processed data of a child without lawful basis, it will delete such data promptly.

20. Marketing and Communications

20.1 **Operational Communications**
PAY247 may send service, transaction, or policy-related messages that are not promotional in nature.

20.2 **Marketing to Merchants**
We may send limited B2B marketing communications (e.g., product updates or new feature announcements) to registered Merchant contacts based on legitimate interest.

20.3 **Opt-Out**
Recipients may opt out at any time by following the unsubscribe link or contacting **privacy@pay247.io**. Opt-out does not affect service notifications necessary to operate your account.

20.4 **Third-Party Marketing**
PAY247 does not sell or provide Personal Data to third parties for their independent marketing.

21. Third-Party Links, Integrations, and Business Transfers

21.1 **Third-Party Links**
PAY247's websites or dashboards may contain links to third-party websites. We are not responsible for their privacy or security practices. Users should review those sites' own privacy policies.

21.2 **Third-Party Services**
When Merchants integrate third-party plugins, payment methods, or analytics tools, those providers act as independent controllers for their data collection.

21.3 **Business Transfers**
If PAY247 is involved in a merger, acquisition, restructuring, or sale of assets, Personal Data may be transferred as part of that transaction. Any successor will continue to protect data under terms consistent with this Policy.

22. Business Continuity, Mergers, and Corporate Restructuring

22.1 **Continuity of Protection**
If PAY247 undergoes a merger, acquisition, restructuring, financing, or sale of all or part of its business, Personal Data may be transferred as part of the transaction. Such transfers will maintain protections materially equivalent to those described in this Policy.

22.2 **Notification of Change**
Where required by law, PAY247 will notify affected individuals or Merchants before Personal Data is transferred to a new owner or becomes subject to a materially different privacy policy.

22.3 **Successor Obligations**
Any successor entity assumes the rights and obligations of PAY247 under this Policy and will honour all active consents, restrictions, and retention commitments.

23. Exercising Rights and Complaints

23.1 **Submitting a Request**
Individuals wishing to exercise their rights (as described in Section 16) or raise privacy-related concerns may submit a request to:

privacy@pay247.io
or by post to the address in Section 25.

23.2 **Identity Verification**
For security, PAY247 may request sufficient information to verify the requester's identity and relationship to the data before acting on any request.

23.3 **Authorised Agents**
Where permitted by law (e.g., under the CPRA), an authorised agent may act on behalf of an individual by providing written authorisation and verification documents.

23.4 **Complaints to Authorities**
If you believe your rights have been violated, you may lodge a complaint with your local data-protection authority or with:
Office of the Information Commissioner, British Virgin Islands
[official website URL once operational]
PAY247 will cooperate fully with competent authorities in investigating and resolving such complaints.

23.5 **Response and Resolution**
PAY247 aims to acknowledge all complaints within 7 Business Days and resolve them within 30 Business Days where practicable.

24. Updates to this Policy

24.1 **Revision Frequency**
PAY247 reviews this Policy at least annually or whenever legal, regulatory, or operational changes materially affect its data-processing practices.

24.2 **Notice of Changes**
Material updates will be communicated by email, dashboard notice, or website publication at https://www.pay247.io/legal/privacy with a revised "Effective Date."

24.3 **Acceptance of Changes**
Continued use of the Services after an update's effective date constitutes acceptance of the revised Policy. If you disagree with any material change, you may cease using the Services and request deletion of your data where permitted.

24.4 **Archival Copies**
Previous versions will be retained for regulatory audit and transparency.

25. Contact Information and Regulatory References

25.1 **Primary Contact**
Anytime Technologies Limited (trading as PAY247)
Attn: Privacy and Compliance Department
Asia Leading Chambers, Road Town, Tortola, VG1110
British Virgin Islands
privacy@pay247.io

25.2 **European and UK Representatives**
Where required under Articles 27 EU / UK GDPR, PAY247 will designate a representative. The representative's contact details will be available on the company's legal page.

25.3 **Supervisory Authorities**

- **British Virgin Islands:** Office of the Information Commissioner

- **EU Data Subjects:** Local Supervisory Authority (e.g., CNIL, DPA, or AEPD)
- **UK Data Subjects:** Information Commissioner's Office (ICO)
- **U.S. Residents:** State Attorney General or California Privacy Protection Agency, as applicable
- **Brazil:** Autoridade Nacional de Proteção de Dados (ANPD)
- **Singapore:** Personal Data Protection Commission (PDPC)
- **India:** Data Protection Board of India

25.4 **Language and Interpretation**
This Policy is drafted in English. Translations are provided for convenience only; in the event of inconsistency, the English version prevails.

25.5 **Changes to the Privacy Policy**

We may update this Privacy Policy from time to time. Any changes will be posted on the Website and will take effect on the date they are published.