CROSS-BORDER DATA TRANSFER CONSENT

Company Information:
FYSM Market FZC LLC
License No.: 4414135.01
Address: Business Centre, Sharjah Publishing City Free Zone, Sharjah, UAE
Email: fysmmarket@gmail.com

1. Introduction

This Cross-Border Data Transfer Consent ("Consent") forms an integral part of the Terms of Service and Privacy Policy of FYSM Market FZC LLC ("Company," "we," "us," or "our"). This Consent is provided in compliance with UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data and its implementing regulations.

2. Purpose of Cross-Border Data Transfer

The Company conducts its commercial operations on a global scale, necessitating the transfer of your personal data beyond the territorial jurisdiction of the United Arab Emirates to various international jurisdictions. This cross-border data transfer is conducted for specified, explicit, and legitimate purposes, in accordance with Article 5 of UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data. The primary purposes justifying such international data transfers include, but are not limited to, the following operational requirements:

2.1. International Order Processing and Logistics Fulfilment

Your personal data, including but not limited to recipient identification information, delivery addresses, and contact details, will be transferred to our international logistics partners, warehouse facilities, and customs brokerage services located in various countries to enable the physical delivery of purchased products to your specified international destination. This transfer is essential for customs declaration processing, shipping label generation, delivery coordination, and providing real-time tracking updates across different jurisdictions.

2.2. Global Payment Processing Operations

To facilitate secure financial transactions for your purchases, your payment information and related transaction data will be transmitted to internationally recognized payment gateway providers, acquiring banks, and financial institutions located outside the UAE. These transfers are necessary for payment authorization, fraud detection and prevention, currency conversion processing, and compliance with international financial regulations and anti-money laundering protocols.

2.3. Customer Support Service Delivery

Your customer service inquiries, account information, and communication history may be processed through our global customer support centers and service providers located in various countries to ensure continuous, around-the-clock support availability. This enables efficient handling of customer queries, technical support requests, and service-related communications across different time zones and linguistic requirements.

2.4. Marketing and Analytics Operations

Personal data related to your browsing behavior, purchase history, and product preferences may be transferred to our international marketing partners and analytics service providers for the purposes of market analysis, customer segmentation, personalized marketing communications, and performance measurement of our global marketing campaigns, in accordance with your marketing preferences and consent selections.

2.5. Cloud Infrastructure and Data Management

Your personal data will be stored and processed through our globally distributed cloud computing infrastructure and data centers located in various international jurisdictions. This transfer enables robust data security, disaster recovery capabilities, system redundancy, and efficient data management practices while maintaining appropriate technical and organizational measures to safeguard your information.

2.6. International Legal and Regulatory Compliance

In certain circumstances, we may be required to transfer your personal data to international regulatory authorities, law enforcement agencies, or judicial bodies in compliance with legal obligations arising from international treaties, mutual legal assistance agreements, or legitimate requests from foreign governmental authorities made through proper legal channels.

3. Types of Personal Data Transferred

In the course of our global business operations, specific categories of your personal data may be transferred internationally. Each data category is processed and transferred in accordance with the principles of data minimization and purpose limitation as stipulated in UAE Federal Decree-Law No. 45 of 2021. The comprehensive classification of personal data subject to cross-border transfer encompasses the following detailed categories:

3.1. Identity and Contact Information

This category comprises core personal identifiers and communication details essential for service delivery, including:

- Complete legal name, including given names and surnames;
- Physical delivery addresses and associated location details;
- Active electronic mail addresses for order confirmations and service communications;
- Verified telephone numbers for delivery coordination and security verification;
- Secondary contact information for emergency delivery scenarios.

3.2. Commercial Transaction Data

Detailed records of your commercial interactions with our enterprise, including:

- Comprehensive order specifications with itemized product selections;
- Complete purchase history with transactional timestamps and value;
- Shipping method selections and associated cost calculations;

- Return and exchange request records where applicable;
- Service usage patterns and subscription management data.

3.3. Financial Transaction Information

Secure payment processing data handled through encrypted channels:

- Payment card details (encrypted and tokenized) including card type and expiration;
- Digital wallet identifiers and transaction authorization tokens;
- Billing address verification and validation information;
- Transaction audit trails for financial reconciliation;
- Fraud detection parameters and risk assessment scores.

3.4. Customer Interaction Records

Documented history of all service-related communications:

- Customer support ticket submissions and resolution records;
- Electronic mail correspondence threads with timestamps;
- Live chat transcripts and voice call recordings (where applicable);
- Service feedback submissions and satisfaction survey responses;
- Technical support inquiries and troubleshooting documentation.

3.5. Digital Footprint and Technical Identifiers

Automatically collected technical information from digital interactions:

- Internet Protocol (IP) addresses and geographical location approximations;
- Device specifications including hardware identifiers and operating system details;
- Browser characteristics with version information and configuration settings;
- Cookie identifiers and tracking technology data (as per Cookie Policy);
- System performance metrics and error log information.

3.6. Behavioral and Preference Data

Information derived from your engagement with our services:

- Product browsing history and search query patterns;
- Wish list compositions and saved item selections;
- Content engagement metrics and interaction heatmaps;
- Marketing communication responsiveness and engagement rates;
- Personalization settings and user interface preferences.

Each data category is transferred only to the extent necessary to fulfill the specific purposes outlined in this Consent, with appropriate technical and organizational measures implemented to ensure the security and confidentiality of your personal data throughout the international transfer process.

4. Destination Countries

4.1. Global Service Provider Network Locations

Your personal data may be systematically transferred to and processed in countries and jurisdictions where our authorized service providers, subcontractors, and strategic partners maintain their primary operations or data processing facilities. These entities include, but are not limited to, international payment processors, customer relationship management platform providers, enterprise resource planning system hosts, and specialized service vendors that support our global business operations. The selection of these service providers is contingent upon their demonstrated compliance with international data protection standards and their implementation of adequate security measures as mandated by applicable data protection regulations.

4.2. Cloud Infrastructure and Data Hosting Geography

Our organization utilizes globally distributed cloud computing infrastructure and data center facilities spanning multiple international jurisdictions. Your personal data may be systematically stored, backed up, and processed within these geographically dispersed facilities to ensure operational resilience, disaster recovery capability, and optimal service performance. Primary cloud hosting locations may include, but are not restricted to, territories within North America, the European Economic Area, the Asia-Pacific region, and emerging digital infrastructure hubs that meet our stringent security and reliability requirements.

4.3. Logistics and Supply Chain Partner Countries

To facilitate international order fulfillment and delivery services, your personal data, specifically delivery and customs information, will be necessarily transferred to countries within our global logistics network. These jurisdictions include the destination country of your shipment, transit hubs through which your package may travel, and the operational centers of our logistics partners involved in the transportation and customs clearance process. This transfer is essential for completing customs declarations, coordinating last-mile delivery services, and providing comprehensive shipment tracking across international borders.

4.4. Specified Jurisdictions with Established Operations

Based on our current operational footprint and strategic business relationships, your personal data may be routinely transferred to, stored in, and processed within specifically identified jurisdictions that include, without limitation:

- The United States of America, where many of our core technology providers and platform infrastructure are headquartered;
- Member states of the European Union, particularly those where we maintain strategic partnerships and compliant data processing arrangements;

- The Republic of India, where certain operational support functions and technical services may be performed;
- Additional jurisdictions where we maintain local entities, branch offices, or established operational presence to support our global customer base.

4.5. Dynamic Jurisdictional Transfers

The global nature of our business operations may necessitate ad-hoc transfers of personal data to other jurisdictions not specifically enumerated herein, particularly in circumstances involving specialized service requirements, emergency operational needs, or the engagement of new international partners. In all such cases, transfers will be conducted in strict compliance with applicable data protection regulations, implementing appropriate safeguards as required by governing legislation, including the utilization of standard contractual clauses, binding corporate rules, or other approved transfer mechanisms where necessary to ensure continued protection of your personal data.

5. Data Protection Measures

5.1. Regulatory-Compliant Transfer Mechanisms

The Company implements and maintains internationally recognized legal frameworks for cross-border data transfers, ensuring compliance with UAE Federal Decree-Law No. 45 of 2021 and other applicable international data protection regulations. Our primary safeguard mechanism incorporates the systematic implementation of Standard Contractual Clauses (SCCs) as approved by relevant data protection authorities, including the European Commission and UAE Data Office. These binding contractual instruments are integrated into all our international data processing agreements, establishing mandatory data protection obligations that travel with the data regardless of jurisdiction, thereby ensuring continuous protection throughout the data lifecycle.

5.2. Comprehensive Third-Party Governance Framework

We establish and enforce rigorous data processing agreements (DPAs) with all third-party providers, subcontractors, and strategic partners involved in handling personal data. These comprehensive DPAs specify detailed obligations regarding data processing limitations, purpose specification, security requirements, and breach notification protocols. The agreements explicitly prohibit unauthorized further transfers, mandate immediate notification of data breaches, and establish clear liability arrangements. We maintain a centralized register of all data processors, regularly verifying their compliance with these contractual obligations through systematic monitoring and assessment procedures.

5.3. Multi-Layered Technical Security Architecture

Our organization implements a defense-in-depth technical security strategy that incorporates multiple layers of protection, including:

- **Encryption Protocols**: Implementation of industry-standard encryption mechanisms including AES-256 for data at rest and TLS 1.3+ for data in transit, with robust key management practices and regular cryptographic reviews.

- **Access Control Systems**: Role-based access control (RBAC) matrices, principle of least privilege enforcement, multi-factor authentication requirements, and privileged access management solutions for all systems handling personal data.
- **Network Security Measures**: Next-generation firewalls, intrusion detection and prevention systems, distributed denial-of-service protection, and comprehensive network segmentation to isolate sensitive data environments.
- **Pseudonymization Techniques**: Systematic implementation of data pseudonymization where appropriate, ensuring the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional separately stored information.

5.4. Organizational Security Measures and Governance

We maintain a structured organizational security framework that includes:

- **Security Awareness Programs**: Regular, role-specific data protection training for all employees and contractors, with particular emphasis on personnel handling cross-border data transfers.
- **Data Protection by Design and Default**: Systematic integration of data protection principles into all business processes, systems, and product development lifecycles through Privacy Impact Assessments and Data Protection Impact Assessments.
- **Incident Response Preparedness**: Comprehensive data breach response plans, regularly tested through tabletop exercises and simulation scenarios, ensuring prompt notification to regulatory authorities and affected individuals where required.
- **Physical Security Controls**: Advanced physical access controls, environmental protections, and monitoring systems for all facilities housing personal data processing infrastructure.

5.5. Continuous Assurance and Compliance Verification

The Company maintains an ongoing program of security assessments and audits to validate the effectiveness of our data protection measures, including:

- **Regular Security Assessments**: Quarterly vulnerability assessments and penetration testing conducted by internal security teams and independent third-party specialists.
- **Compliance Audits**: Annual comprehensive audits against international standards including ISO 27001, SOC 2, and applicable data protection regulations.
- **Third-Party Risk Management**: Systematic evaluation of all vendors and partners through security questionnaires, on-site audits where necessary, and continuous monitoring of their security posture.
- **Internal Control Reviews**: Biannual reviews of internal data protection controls, policies, and procedures by our internal audit function and Data Protection Officer.

This comprehensive framework of technical and organizational measures ensures that personal data transferred across international borders receives protection equivalent to that required under UAE law, regardless of the jurisdiction in which it is processed.

6. Third-Party Recipients

6.1. Global Logistics and Shipping Partners

To facilitate worldwide delivery of products, your personal data will be shared with our network of international logistics and shipping partners. These entities include global courier services, freight forwarders, customs brokerage firms, and last-mile delivery providers. The specific data elements shared with these partners are limited to: recipient identification information (complete name), detailed delivery address, contact telephone number, and email address for shipping notifications. Additionally, these partners receive necessary customs declaration information including, but not limited to, product descriptions, declared values, and harmonized system codes as required by international trade regulations.

6.2. Financial Services and Payment Processing Entities

Your payment and transaction data will be securely transmitted to authorized financial institutions and payment service providers. These entities include: international acquiring banks, payment card processors, digital wallet providers, and fraud detection service providers. The data shared with these entities is strictly limited to: payment instrument details (encrypted), transaction amounts, billing address information, and device fingerprinting data for fraud prevention purposes. All payment processors in our network maintain PCI DSS Level 1 certification and implement tokenization technologies to minimize data exposure.

6.3. Customer Engagement and Relationship Management Providers

To ensure consistent and personalized customer experiences, your interaction data may be processed through our customer relationship management (CRM) ecosystem. This includes: cloud-based CRM platform providers, customer service software vendors, helpdesk system operators, and customer communication management services. The data elements accessible to these providers include: complete contact information, purchase history, customer service interaction records, communication preferences, and service usage patterns, all protected through robust access controls and encryption mechanisms.

6.4. Analytics and Marketing Technology Partners

For business intelligence and customer engagement purposes, certain data may be shared with our analytics and marketing partners. These include: web analytics service providers, marketing automation platforms, advertising technology companies, and customer data platform operators. The data shared with these entities typically includes: pseudonymized identifiers, browsing behavior patterns, campaign interaction data, product interest indicators, and aggregated performance metrics. All marketing partners are contractually required to implement appropriate data minimization and privacy protection measures.

6.5. Cloud Infrastructure and Technology Service Providers

Your data is stored and processed through our enterprise cloud infrastructure partners, including: infrastructure-as-a-service providers, platform-as-a-service operators, software-as-a-service vendors, and managed service providers. These entities provide the technical foundation for our global operations and may have access to personal data as necessary to perform their designated functions. All cloud providers undergo rigorous

security assessments and maintain internationally recognized certifications including ISO 27001, SOC 2, and CSA Star attestation.

6.6. Legal, Regulatory and Governmental Authorities

In specific circumstances, we may be obligated to disclose personal data to: law enforcement agencies, regulatory bodies, judicial authorities, and other governmental entities. Such disclosures occur only when: required by applicable laws or regulations, necessary to respond to valid legal process, essential to protect our rights and property, or urgently needed to ensure the safety of our customers and the public. In all such cases, we carefully review the legitimacy of the request and minimize the disclosure to only what is legally required.

All third-party recipients are subject to comprehensive due diligence assessments and are contractually bound to implement equivalent data protection standards as those maintained by our organization. We maintain a centralized register of all data processors and regularly review their compliance with our data protection requirements.

7. Your Rights

7.1. Comprehensive Rights Framework

In accordance with UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data and its implementing regulations, you possess specific rights regarding your personal data. The Company has established a comprehensive framework to facilitate the exercise of these rights, ensuring transparency and accountability in our data processing activities.

7.2. Right to Withdraw Consent

You maintain the absolute right to withdraw your consent for the processing of your personal data at any time, without affecting the lawfulness of processing based on consent before its withdrawal. The withdrawal process can be initiated through our dedicated privacy portal or by submitting a formal written request to our Data Protection Officer. Upon receipt of your withdrawal request, we will cease processing your personal data for the purposes covered by the consent within a maximum of fifteen (15) business days, unless alternative legal bases for processing exist.

7.3. Right of Access and Information

You have the right to obtain confirmation as to whether or not personal data concerning you are being processed, and where that is the case, access to the personal data and specific information including: the purposes of processing, categories of personal data concerned, recipients or categories of recipients to whom the personal data have been or will be disclosed, the envisaged period for which the personal data will be stored, and the existence of automated decision-making, including profiling.

7.4. Right to Rectification and Data Accuracy

You are entitled to request the rectification of inaccurate personal data concerning you without undue delay. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement. We have implemented technical and organizational measures to

ensure the ongoing accuracy and currency of your personal data throughout our processing activities.

7.5. Right to Erasure ("Right to be Forgotten")

Subject to specific conditions outlined in Article 16 of UAE Data Protection Law, you have the right to obtain the erasure of personal data concerning you without undue delay when: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent on which the processing is based; you object to the processing and there are no overriding legitimate grounds for the processing; or the personal data have been unlawfully processed.

7.6. Right to Object to Processing

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on legitimate interests or the performance of a task carried out in the public interest. The Company shall no longer process the personal data unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

7.7. Right to Data Portability

You have the right to receive the personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from us, where: the processing is based on consent or on a contract; and the processing is carried out by automated means. This right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

7.8. Rights Exercise Procedure

To exercise any of these rights, you may submit a verifiable request to us by either:

- Emailing our Data Protection Officer at fysmmarket@gmail.com;
- Using the dedicated rights portal within your account dashboard;
- Submitting a written request to our registered office address.

We will respond to all legitimate requests within thirty (30) days of receipt, with a possible extension of an additional thirty (30) days for complex requests, in which case we will notify you of the extension within the initial thirty-day period.

8. Withdrawal of Consent

You may withdraw your consent for cross-border data transfers by contacting us at fysmmarket@gmail.com. However, please note that withdrawal of consent may affect our ability to provide you with our products and services, particularly international shipping and payment processing.

9. Data Retention

We retain your personal data only for as long as necessary to fulfill the purposes outlined in this Consent, unless a longer retention period is required or permitted by law.

10. Contact Information

For questions, concerns, or requests regarding this Cross-Border Data Transfer Consent, please contact:

Data Protection Officer

FYSM Market FZC LLC
Business Centre, Sharjah Publishing City Free Zone
Sharjah, United Arab Emirates
Email: fysmmarket@gmail.com

ACKNOWLEDGEMENT AND CONSENT

By using our website, placing orders, or providing your personal data, you acknowledge that you have read and understood this Cross-Border Data Transfer Consent and expressly consent to the transfer, storage, and processing of your personal data outside the United Arab Emirates as described herein.

Date of Last Update: 22.09.2025