GLOBAL KYC & DATA PROCESSING CONSENT ADDENDUM

Issued by: Vindex Legal Risk Ltd, UK

This Global Know Your Customer (KYC) & Data Processing Consent Addendum ("Addendum") establishes the worldwide legal framework under which **Vindex Legal Risk Ltd, UK** (the "Company") collects, processes, verifies, cross-references, and stores personal data and sensitive identifying information for compliance verification purposes.

1. Global Authorization, Consent & Purpose

By signing this Addendum, I hereby provide my **explicit, voluntary, specific, and unambiguous consent** to the Company to collect, process, and securely verify my personal data. This includes, but is not limited to, my full name, date of birth, nationality, passport copies, identification card details, facial biometrics, and verified proof of address. This processing is performed solely to fulfill mandatory **Know Your Customer (KYC)**, Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and corporate regulatory screening requirements worldwide.

2. Worldwide Scope & Regional Legal Declarations

This framework operates as a universal global baseline. Where specific country or regional data protection regimes apply, the following statutory requirements are incorporated directly into this consent:

- **United Kingdom & European Union:** Processing is explicitly grounded on UK/EU GDPR Article 6(1)(a) (Consent) and Article 6(1)(c) (Legal Obligation) to fulfill local Money Laundering Regulations. Cross-border transfers outside the EEA or UK utilize approved Standard Contractual Clauses (SCCs) and International Data Transfer Agreements (IDTAs).
- **United States:** Information is collected, verified, and handled to satisfy Customer Identification Program (CIP) obligations under the Bank Secrecy Act and USA PATRIOT Act, adhering to state-specific privacy rules where applicable.
- **Australia:** Processing complies with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth) and identity verification standards mandated by AUSTRAC under the AML/CTF Act 2006.
- **Canada:** Explicit consent is established in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial private-sector legislation, meeting identity verification benchmarks required by FINTRAC.
- **South America (including Brazil & Argentina):** Processing aligns with Brazil's Lei Geral de Proteção de Dados (LGPD) Article 7(I) and Argentina's Personal Data Protection Act No. 25.326, fulfilling cross-border data transfer validations and international compliance duties.
- **India:** This document serves as valid, clear notice and consent under the Digital Personal Data Protection (DPDP) Act, 2023. Processing satisfies the Prevention of Money-Laundering Act (PMLA) rules.
- **Singapore & Malaysia:** Formulated in strict compliance with the Singapore Personal Data Protection Act (PDPA), Monetary Authority of Singapore (MAS) AML/CFT Notices, and the Malaysian Personal Data Protection Act 2010.

- **China:** Pursuant to the Personal Information Protection Law (PIPL), the individual provides separate, explicit consent for the cross-border processing of sensitive personal information (passport datasets and identity verification profiles).
- **Kazakhstan:** This document satisfies the mandatory written consent framework required for processing and international transfer under Law No. 94-V 'On Personal Data and their Protection'.
- **Rest of the World (Global Baseline):** For countries not listed explicitly above, this consent functions as a comprehensive, voluntary contractual authorization satisfying standard local data validation laws and compliance audits.

3. Confidentiality, Security & Breach Notification Protocol

The Company enforces strict technical, physical, and organizational security mechanisms to protect all sensitive personal records against unauthorized access, loss, or disclosure. In the event of a confirmed data breach impacting your personal information, the Company maintains a strict incident management policy. Notifications will be provided transparently to affected data subjects and appropriate governing watchdogs—such as the **UK Information Commissioner's Office (ICO)** and corresponding international regulators—in strict accordance with statutory reporting windows.

4. Regulatory Data Retention Policy

To satisfy binding global financial screening audits, statutory anti-money laundering records mandates, and international regulatory requirements, all collected passport records, identity profiles, screening transcripts, and verification histories will be securely retained for a firm period of **seven (7) years** following the formal termination of the business relationship. Upon expiration of this period, data will be permanently destroyed or anonymized.

5. Data Subject Rights & Contact Information

Depending on your geographic location, you hold distinct rights regarding your personal information, including the right to access, rectify, restrict processing, or request erasure (subject to the 7-year regulatory retention exception). For all inquiries, compliance requests, or to exercise your legal data privacy rights, you may contact the Company's dedicated privacy desk directly at: **privacy@vindexlegalrisk.com**.

Execution & Acknowledgment Block

By executing this document below, I acknowledge that I have read, understood, and agreed to the global collection, processing, cross-border transfer, and regulatory retention terms outlined in this Addendum.

Client Full Name: _____

Passport / National ID Number: _____

Country of Residence: _____

Signature: _____

Date: _____