

# ACCEPTABLE USE POLICY


## DMA LINK LIMITED

Version 1.0

This **Acceptable Use Policy** forms part of our CDD, AML, CFT Procedure dated 11 August 2023, which is available online at [dmlink.com/kyc](https://dmlink.com/kyc).

Access to the platform is governed by our Terms, accessible on our legal repository [dmlink.com/agreement](https://dmlink.com/agreement).

**Document Particulars.** Refer to the table below.

|                         |   |           |   |
|-------------------------|---|-----------|---|
| Document Title          | Acceptable Use Policy   |           |   |
| Documents Code          | AUP2024   |           |   |
| Owner(s)                | Board of Directors  |           |   |
| Administrator(s)        | Compliance Officer (“CO”) and Money Laundering Reporting Officer (“MLRO”) |           |   |
| Created Date (Original) | 19 April 2024   |           |   |
| Department              | Management  |           |   |
| Users                   | All directors, employees, agents, contractors, consultants                |           |   |
| Revision                | 1.0   |           |   |
| Revision Date           | NA  |           |   |
| Amendments By           | Ashwind Soonarane (COO)   | Signature |  |

DMA LINK LIMITED  
 71-75 SHELTON STREET  
 LONDON WC2H 9JQ  
 LEGAL@DMALINK.COM  
 WWW.DMALINK.COM

## 1. Scope

- 1.1. This Acceptable Use Policy (“Policy”) is applicable to all Clients of DMA LINK LIMITED, including you (“the Client”) and it forms an integral part of our CDD, AML, CFT Procedure dated 11 August 2023, available online at [dmlink.com/kyc](https://dmlink.com/kyc).
- 1.2. DMA LINK LIMITED expects Clients to adhere to the spirit and the letter of applicable laws, regulations, good industry practices and international standards in financial crime risk management, where the Client operates.
- 1.3. Clients must comply with the requirements of this Policy at all times.
- 1.4. This Policy forms part of the terms and conditions you entered into with DMA LINK LIMITED for the use of its products and services (as amended from time to time).
- 1.5. If there is any inconsistency or conflict between this Policy and any other part of the applicable DMA LINK LIMITED terms and conditions, the latter shall take priority and prevails unless DMA LINK LIMITED specifies otherwise.

## 2. Requirements

- 2.1. DMA LINK LIMITED conducts stringent customer due diligence (“CDD”) measures, ongoing monitoring, and enhanced due diligence (“EDD”) where required, on all business relationships with Clients.
- 2.2. As part of these measures, Clients will be required to share with DMA LINK LIMITED information about its own organisation, business model, operation model, customer base, and financial crime compliance systems and controls, where applicable and requested. The extent of the CDD, ongoing monitoring and EDD measures will be solely determined by DMA LINK LIMITED on a risk-sensitive basis, depending upon the type of Client, business model, regulatory landscape, product and transactions.
- 2.3. DMA LINK LIMITED may impose conditions and/or restrictions to commence or continue providing products and services to Clients. This includes restrictions on activities and/or transactions, as well as requesting the Client to cease and desist particular activities and not using the DMA LINK LIMITED Platform in relation to certain counterparties and jurisdictions.

24. DMA LINK LIMITED may not be able to disclose the reasons behind such restrictions and cease and desist requests in order for DMA LINK LIMITED to comply with applicable law.
25. To comply with applicable money laundering regulations, DMA LINK LIMITED may also request information about the intended purpose and nature of certain transactions in the DMA LINK LIMITED Platform by means of a request for information (“RFI”). It is important that Clients provide DMA LINK LIMITED with complete responses to the requests to avoid delaying any transactions and to help general efficiency with its processes.

### 3. Financial Crime Risk Management

31. Based on the activities of a Client, DMA LINK LIMITED may require a Client to establish and maintain policies, controls and procedures to mitigate and manage effectively the Client’s risks of financial crime which the Client has identified in its documented risk assessments. These policies, controls and procedures should cover at minimum: risk management practices; internal controls; customer due diligence activities; reporting and record-keeping; and monitoring and management of compliance with, and the internal communication of, such policies, controls and procedures. DMA LINK LIMITED expects that the Client’s controls are adequate to the nature, scale, size and complexity of the Client’s business, and must provide assurance that the Client will not violate applicable laws and regulations and/or pose an unacceptable level of financial crime or other regulatory compliance risk.
32. Based on the activities of a Client, DMA LINK LIMITED may require a Client to conduct EDD and enhanced ongoing monitoring of situations and circumstances prescribed by applicable law and regulations. Where Clients are unable to apply CDD measures to an underlying customer/end-user, the Client must:
  - 32.1. not carry out a transaction through the DMA LINK LIMITED Platform or via any partner of DMA LINK LIMITED or on behalf of the customer; and
  - 32.2. consider whether it ought to be making a report to the law enforcement, in accordance with its obligations under applicable law for money laundering and terrorism financing.
33. Where a Client has concluded that the payments processed via the DMA LINK LIMITED Platform gives reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, and the matter has been reported to the

relevant law enforcement agency, DMA LINK LIMITED expects you to cease and desist all future activities, via the DMA LINK LIMITED Platform or any partner of DMA LINK LIMITED, relating to the person or company for which the Client has knowledge or suspicion about.

## 4. Prohibited Relationships

- 4.1. DMA LINK LIMITED will not establish business relationships with and requires the Client not to enter into relationships with the following prohibited entities and individuals, which include:
  - 4.1.1. entities who provide anonymous accounts, numbered accounts or accounts in fictitious names;
  - 4.1.2. shell banks;
  - 4.1.3. shell companies with no independent operations, significant assets, ongoing business activities and/or employees;
  - 4.1.4. bearer share companies and those operating as such;
  - 4.1.5. individuals or entities subjected to financial sanctions by applicable law and/or regulation;
  - 4.1.6. entities and individuals located in the countries included in the Appendix I; and,
  - 4.1.7. entities included in the Appendix II.

## 5. Prohibited Transactions

- 5.1. The DMA LINK LIMITED Platform or any of DMA LINK LIMITED's partners must not be used to initiate and/or receive payments with the following characteristics:
  - 5.1.1. payments that appear to relate to any form of illegal and/or unlawful activity, including, but not limited to, money laundering, terrorist financing, trade based money laundering, fraud, bribery and corruption, sanctions evasion, ransomware, human trafficking and illegal wildlife trafficking;

- 5.1.2. payments to which you are required to hold a regulatory permission, including a license granted by a local financial authority and/or appointed representatives and agents;
- 5.1.3. payments that are sanctioned and/or involving designated persons according to the United Kingdom, European Union, United Nations and the United States;
- 5.1.4. payments to and from the countries listed in Appendix I;
- 5.1.5. payments involving the industries listed in Appendix II;
- 5.1.6. payment involving shell companies with no independent operations or significant assets or ongoing business activities or employees;
- 5.1.7. payments that do not appear to have a legitimate purpose, including but not limited to payments/transactions in repetitive, round amounts and payments lacking transparency regarding the originator/payer and beneficiary/payee;
- 5.1.8. payments that involve the use of an informal value transfer system<sup>1</sup>;
- 5.1.9. payments that appear to circumvent currency controls;
- 5.1.10. payments involving unregulated/unauthorised money or value transfer service providers, including money service businesses (“MSB”)<sup>2</sup>;
- 5.1.11. payments involving illegal gambling, including remotely<sup>3</sup>;
- 5.1.12. payments involving cryptoasset exchange providers or custodian wallet providers that are not duly licensed and not domiciled in a financial action task force member country;
- 5.1.13. transactions involving crypto ATM offering cryptoasset exchange services that are not duly licensed;

---

<sup>1</sup> *Informal value transfer system (“IVTF”) – An “informal value transfer system” refers to any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form. IVTS include various ethnic traditions or practices, such as hawala, hundi, padala, fei chien, Phoe kuan, and the black market peso exchange. Most of them have also been referred to as ‘underground banking systems’ or ‘alternative remittance systems’.*

<sup>2</sup> *Money or value transfer services (“MVTs”) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTs provider belongs.*

<sup>3</sup> *For the purposes of the Policy, ‘gambling’ means gaming, betting, lottery, casino. ‘Remote*

*gambling' means gambling in which persons participate by the use of remote communication.*

- 5.1.14. payments involving third-party payment processors that resell their services to a third party or payments related to the provision of correspondent banking services to other financial institutions (also known as, nesting or downstream correspondent banking services), which is not approved by DMA LINK LIMITED in writing and that do not have appropriate anti-money laundering/counter terrorism financing and sanctions compliance programs in place;
- 5.1.15. payments associated with payable-through accounts<sup>4</sup>; and
- 5.1.16. payments involving shell banks.

## 6. Failure to Comply

- 6.1. Failure of a Client to comply with this Policy will constitute a breach of the DMA LINK LIMITED terms and conditions.
- 6.2. Any breach of this Policy may result in DMA LINK LIMITED exercising its right to suspend or terminate the DMA LINK LIMITED terms and conditions.

---

<sup>4</sup> According to the Wolfsberg Group - payable through account involves a respondent FI opening an account with a correspondent FI and then providing its customers with means of drawing directly on the respondent's account with the correspondent. The risk is that the Indirect Customer is dealing directly with the Correspondent without any transactional control being applied by yourself, opening the Correspondent to potential regulatory breaches.

## Appendix I - Prohibited Countries and Regions

Belarus, Cuba, Democratic People's Republic of Korea (DPRK), Islamic Republic of Iran, Russian Federation, Syria, Crimea, Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) regions of Ukraine

## Appendix II – Prohibited Industries

| Group  | Industry  |
|--|---|
| Adult  | Escort / Sex workers advertising                            |
|  | Pornographic video sharing and pornography website          |
| Arms and Defense                               | Manufacture of military fighting vehicles                   |
|  | Manufacture of weapons and ammunition                       |
| Cash Intensive Business and High Value Dealers | Cash and Valuables-in-Transit                               |
|  | Scrap Metals Dealers / Warehouse                            |
| Cryptocurrency business                        | Virtual Currency Administrators or Miners                   |
|  | Unlicensed VC exchange                                      |
| Financial Services                             | Shell Banks   |
|  | Unlicensed MSB, or similar money or value transfer services |
|  | Informal Value Transfer System (FINCEN definition)          |
| Gambling Business                              | Unlicensed Gambling business (remote and non-remote)        |
| Wildlife                                       | Wildlife - Illegal Wildlife Trade                           |