

ANTI-MONEY LAUNDERING (AML), COUNTER-TERRORIST FINANCING (CTF) AND ANTI-BRIBERY & CORRUPTION POLICY STATEMENT

Money laundering and terrorist financing have been identified as a major threat to the international financial services community. Many countries have passed therefore legislation designed to prevent money laundering and to combat terrorism. This legislation, together with regulations, rules and industry guidance, form the cornerstone of AML/CTF obligations for firms and outlines the offences and penalties for failing to comply.

Instinet Germany GmbH ("IGG" or "Instinet" or "the firm"), authorised by the Federal Financial Supervisory Authority (German: Bundesanstalt für Finanzdienstleistungsaufsicht; the BaFin) and regulated by the BaFin and Deutsche Bundesbank, is committed to the highest standards of Anti-Money Laundering (AML), Combatting Terrorist Financing (CTF), Anti-Bribery and Corruption (ABC) and Anti-Financial Crime (FC) and like other entities within the Instinet Group, is responsible for having controls in place in order to comply with local legislation, regulations and any government approved guidance in the jurisdiction(s) in which they operate.

As Germany is a member state of the Financial Action Task Force (FATF) and the European Union, enacted recommendations and laws fully apply to IGG. IGG may have additional local policies and procedures designed to comply with the local legislation, regulations and any government approved guidance in the jurisdiction(s) in which it operates.

Instinet's Policies and Principles:

The responsible Compliance Officer owns and is responsible for the following internal policies covering:

1. Financial Crime Policy Standard (AML / CTF, Sanctions)
2. Anti-Bribery & Anti-Corruption Policy Standard

These policies standards are designed to ensure that IGG complies with the legal and regulatory requirements applicable as well as with any other additional local obligation for regions it may have activities.

Financial Crime

IGG's AML and CTF Policy Standard is designed to ensure that all its European offices comply with the requirements set out under EU legislation, regulations, rules and industry guidance for the financial services sector, including the need to have adequate systems and controls in place to mitigate the risk of the firm being used as a conduit of financial crime.

The Policy Standard is also designed to ensure that the firm complies with applicable sanctions laws in every jurisdiction in which it operates. As such IGG is required to screen against e.g. United Nations, European Sanctions lists as a minimum in all our business dealings.

Anti-Bribery and Corruption

In accordance with its regulatory requirements, IGG is prohibited from inducing a person to perform improperly to gain an advantage or avoid a negative outcome by entering into activity that could constitute a form of bribery. The prevention, detection and reporting of bribery offences are the responsibility of all Instinet staff. Instinet also prohibits any IGG staff to threaten or take action against another IGG staff who has refused to commit a bribery offence or who has raised bribery concerns. Anti-bribery and corruption risks posed to Instinet are limited due to its business

model, and regions of operation, however all staff must constantly assess the application of this policy in their dealings and apply both the spirit and defined rules of this policy when performing their duties.

Governance and Conformance

IGG's policies are endorsed by the Management Board and implemented by the Compliance Department and MLRO. Regular reviews of the effectiveness of these policies are carried out in addition to audits periodically undertaken by both internal and external Auditors.

All employees, contractors, workers and consultants contracting with IGG are required to comply with IGG's Financial Crime Policy Standard and Anti-Bribery & Anti-Corruption Policy Standard.

What does that mean?

To facilitate compliance with anti-money laundering laws, IGG has developed and implemented a comprehensive anti-money laundering and counter terrorist financing programme, consisting of training, policies, procedures and internal systems and controls. This includes, but is not limited to:

- The appointment of a Money Laundering Reporting Officer (MLRO) who is of sufficient seniority, who has the responsibility for oversight of compliance with relevant legislation, regulations, rules and industry guidance;
- Establishing and maintaining a Risk Based Approach (RBA) towards assessing and managing the money laundering and terrorist financing risks of the firm; establishing and maintaining risk-based customer due diligence, identification, verification and Know Your Customer (KYC) procedures. This includes enhanced due diligence for those customers presenting higher risk, such as Politically Exposed Persons (PEPs);
- Establishing and maintaining risk based systems and procedures to monitor ongoing customer activity;
- Procedures for the identification and reporting suspicious activity internally and to the relevant law enforcement authorities as appropriate;
- The maintenance of appropriate records for the minimum periods prescribed by law;
- Training and detailed policies, providing all staff with detailed Financial Crime knowledge;
- The provision of appropriate management information and reporting to senior management of the firm's compliance with the requirements.

European Compliance, October 2020