Inhalt

1. Preamble

Pursuant to § 25h of the German Banking Act (KWG), Middle East Bank, Munich Branch (MB) must, without prejudice to the obligations set out in § 25a (1) of the German Banking Act (KWG) and Sections 4 and 6 of the German Moneylaundering Act (GWG), have internal security measures in place to prevent money laundering, the financing of terrorism or other criminal acts that could endanger the institution's assets. To this end, it must create and update appropriate business and customer-related security systems and carry out controls. This includes the ongoing development of appropriate strategies and safeguards to prevent the misuse of new financial products and technologies for money laundering and terrorist financing purposes or to favour the anonymity of business relationships and transactions. The new version of the **Interpretation and Application Instructions for the Money Laundering Act (AuA)** published by BaFin in January 2018/May 2020 were taken into account in the context of these working instructions. Furthermore, Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, which was passed by the German Bundestag on 12 December 2019, came into force on 1 January 2020. These working instructions serve to implement the statutory and supervisory regulations to combat money laundering and prevent the financing of terrorism. The starting point for all measures is the result of the risk analysis and the risk-based approach to combating money laundering.

At the same time, MB employees are to be sensitised to the problem of money laundering in order to limit the risk of the company or its employees being unintentionally misused for the "laundering" of illegally acquired assets or for the financing of a terrorist organisation. Acts or transactions which are suspected of being involved in money laundering or terrorist financing must therefore always be rejected, without prejudice to the other obligations explained below.

MB shall set up, update and monitor appropriate business and customer-related security systems to prevent money laundering, the financing of terrorism and other criminal acts to the detriment of the institution. The focus is on a risk-oriented approach. The systems and measures must take account of the individual size, organisation and risk situation.

The internal security measures essentially consist of **customer-related due dilligence and the organisational due dilligence**.

2. Internal safeguards - customer due diligence

The **customer-related due diligence obligations are** divided into general due diligence obligations **(Customer Due Diligence (CDD))**, **enhanced customer due diligence (ECDD))** and **simplified customer due diligence (Simplyfied Customer Due Diligence (SCDD)).**

The concrete scope of the measures to be taken in each individual case is to be determined according to the risk of the respective contractual partners, the respective business relationship or the respective transaction. The customer risk is determined before the business relationship is established on the basis of the customer risk categorisation.

The **general due diligence duties** are generally applied to all contractual partners.

Simplified due diligence obligations may be applied where the risk of money laundering or terrorist

financing is low and there is no concrete suspicion of money laundering or terrorist financing. The risk factors listed in Annex 1 to the GWG represent a non-exhaustive list of factors and possible indicators of a potentially lower risk. This is determined and documented within the scope of a customer risk categorisation, taking into account the circumstances of the individual case.

Insofar as there may be increased risks of money laundering or terrorist financing, MB applies additional **increased due diligence obligations** in accordance with § 15 GWG. This is determined and documented within the framework of a customer risk categorisation taking into account the circumstances of the individual case. The list in Annex 2 to § 15 (2) GWG lists corresponding factors and possible indicators of a potentially higher risk.

2.1 Customer Risk Categorization

With the exception of the identification obligation, the general due diligence duties of care are carried out in a risk-oriented manner. The risk-oriented approach is applied throughout the relevant sections of the GWG as a general clause. The customers of MB are categorised in a risk-oriented manner (weighting of risk factors) before the business relationship is established. In doing so, they are classified into one of four risk categories, **"without", "low", "medium" or "high".**

2.2 Identification of natural and legal persons

Natural persons shall be identified by means of a valid official identity document containing a photograph of the holder and which fulfils the passport and identity card requirements in Germany, in particular by means of a passport, identity card or passport or identity card substitute recognised or approved under the law on foreigners. The identity check for **natural Iranian persons** is carried out analogous to the general due diligence obligations, but extended by the increased due diligence obligations.

Legal entities or commercial partnerships are identified on the basis of an extract from the commercial register, an extract from a comparable official register or register, the founding documents or equivalent probative documents or by inspection of register or register data. The identification of **legal Iranian entities** is carried out analogous to the general due diligence obligations, but extended by the increased due diligence obligations.

In accordance with the criteria set out in Article 9 Directive (EU) 2015/849 in conjunction with Regulation (EU) 2016/1675, the EU has determined which Non-EU countries present a higher risk of money laundering or terrorist financing. According to Article 1.II of Regulation 2016/1675 **Iran** is **classified as a Non-EU country with a high risk of money laundering or terrorist financing**. On the basis of this classification, the **enhanced due diligence obligations** apply with regard to the establishment of business relationships with **natural and legal Iranian entities who have their permanent residence in Iran.**

The identification consists of establishing the identity and verifying the identity according to qualified documents.

2.3 Clarification of the beneficial owner

The economic beneficiary is the natural person,

- in whose ownership or control the contracting party is ultimately located,
- at whose instigation a transaction is ultimately carried out or a business relationship is ultimately established, or
- who is mainly the beneficiary of a third-party design.

2.4 Obtaining information on the nature and purpose of the business relationship

When a new business relationship is established, information on the purpose and the intended type of business relationship is obtained and documented as part of the establishment of the business relationship, unless this information is already beyond doubt available from the business relationship.

2.5 Source of funds

MB ensures that transactions undertaken are consistent with the information available on the origin of assets. The clarification of the origin of assets is risk-based, in particular depending on the person of the contractual partner and the type of business relationship. The clarification of the origin of assets is not to be understood as an obligatory routine check. Only the information actually available on the origin of the assets must be taken into account.

2.6 Particularly complex, large or unusual transactions

Transactions that are particularly complex or large in comparison, follow an unusual transaction pattern in the course of the transaction, have no obvious economic or legal purpose, or are a cross-border correspondence relationship with a respondent domiciled in a Non-EU country or in a country of the European Economic Area, have a risk-increasing effect. In this context, increased due diligence obligations are applied.

2.7 Continuous monitoring and obligation to update

sMB continuously monitors the business relationships including the transactions carried out in the course of these relationships. The continuous monitoring begins with the establishment of the business relationship or with the first use of a service or product. It ends when the business relationship is terminated.

2.8 Politically exposed persons

A politically exposed person is any person who holds or has held a high-level important public office at international, European or national level or who holds or has held a public office below national level of comparable political importance. The **FATF** shares this definition of a PEP as a person who is or has been entrusted with a prominent public function and therefore additional AML/CFT safeguards must be applied to business relationships. These measures are preventive and should not be interpreted to mean that all PEPs are involved in criminal activities. The FATF divides PEPs into four categories based on the risks associated with them:

High risk - PEPs Tier 1	**Medium to high level risk - PEPs Tier 2**
• heads of states and governments • Government members (national and regional) • Parliamentarians (national and regional)	• Senior officials of the military, judicial and law enforcement agencies • senior officials of other government departments and bodies and senior officials

• Heads of military, judicial, law enforcement and central bankers • political leaders of political parties	• Older members of religious groups • Ambassadors, Consuls, High Commissioners
Medium risk - PEPs Tier 3 • Management and board of directors of state-owned companies and organisations e.g. chairman of a bank	**Low risk - PEPs Tier 4** • Mayors and members of district, town and county assemblies • senior officials and officials of international or supranational organisations

If there are indicators that the contracting party is a PEP, **the AML Officer will be informed before the business relationship is established.** He will carry out the further clarification measures and determine the scope of the due diligence measures resulting from the PEP status (origin of assets, intensified, continuous monitoring). On the basis of his proposals, the management decides whether to enter into or reject the business relationship.

2.9 Sanctions check

All customers and their beneficial owners are checked against sanction lists before a business relationship with MB can be established.

2.10 Consequences of failure to comply with due diligence obligations

Due to its background and business model, MB follows a conservative approach with regard to the non-execution and termination obligation. If the customer is not in a position to comply with the general due diligence obligations as well as the simplified due diliogence obligations or the enhanced due diligence obligations, the business relationship will not be commenced or continued. If a business relationship already exists, it shall be terminated by the obligor by giving notice, irrespective of any other legal or contractual provisions.

Based on the Bank's compliance culture, all employees are also required to report and document any suspicious situation. The Money Laundering Officer decides together with the management whether to terminate or continue a business relationship or to carry out a transaction.

3. Internal security measures - organisational duties of care

3.1 Money Laundering Officer

The management has appointed a money laundering officer at management level, and a deputy. The Money Laundering Officer is responsible for ensuring compliance with money laundering regulations. He is directly subordinate to the Management Board. The Money Laundering Officer is responsible for all matters relating to compliance with the Money Laundering Act within the institution.

3.2 Risk analysis

The risk analysis is documented and contains the measures to be derived from the risk potential. The decision to take action is taken by the money laundering officer in consultation with the management board.

3.3. Monitoring and control actions

Money laundering related control measures cover all due diligence obligations and take into account existing measures of the bank's internal control system. They are derived from the risk analysis. The money laundering and compliance control actions are mapped and documented in the monitoring and control plan.

3.4. Continuous monitoring of business relationships

MB continuously monitors business relationships including transactions in order to compare customer profiles with their respective transaction behaviour. Dynamic monitoring in this context means taking appropriate account of the findings from the course of the business relationship. If a suspicious transaction is not reported because the initial suspicion cannot be substantiated, the business relationship is subject to monitoring - possibly over a longer period of time - until the doubts are cleared up.

3.5 Suspected cases and their reporting

All facts that indicate that an act pursuant to § 261 StGB or a terrorist financing has been or is being committed or attempted shall immediately trigger a suspicious activity report.

3.6. Regular information of the employees

The Bank conducts regular training courses to inform and educate about the Bank's principles of conduct, guidelines and work instructions. The Bank distinguishes between mandatory classroom training within the first six months and annual and role-based training which is web-based. Employees are instructed at least once a year on the methods of money laundering and terrorist financing and are informed about the obligations under the German Money Laundering Act.

3.7. Reliability of the employees

To ensure the reliability of staff, the Bank applies risk-based measures to verify the reliability of staff before recruitment and in terms of reliability during employment. The Bank only employs staff whose reliability is beyond doubt with regard to the prevention of money laundering and terrorist financing. The Bank does not differentiate between the activities of employees and managers or the classification of areas according to their relevance to money laundering.

3.8. Reporting

At least once a year, the Money Laundering Officer shall report to management on the measures taken, the status of implementation of the obligations arising from the Money Laundering Act, the current risk situation of the institution and significant individual cases.

The Money Laundering Officer shall report immediately on special occurrences, significant individual cases or extraordinary risks.

3.9. Recording and storage obligations

The data collected and information obtained in connection with the due diligence obligations regarding contractual partners, beneficial owners, business relationships and transactions are documented and archived.