Content

1. Preamble

Pursuant to § 25h of the German Banking Act (KWG), Middle East Bank Munich Branch (MB) must have internal safeguards in place to prevent money laundering, terrorist financing or other criminal acts that could endanger the assets of the institution, without prejudice to the obligations listed in § 25a para. 1 KWG and § 4 and 6 GWG. To this end, it must create and update appropriate business and customer-related security systems and carry out controls. This also 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 notes on the Money Laundering Act (AuA)** published by BaFin in January 2018/May 2020 have been taken into account within the scope of this working instruction. 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 adopted by the Bundestag on 12 December 2019, came into force on 1 January 2020. These working instructions serve to implement the statutory and supervisory regulations for combating money laundering and preventing the financing of terrorism. The starting point for all measures is the result of the risk analysis and the risk-based approach in the fight against money laundering.

At the same time, MB employees should be made aware of 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 suspected of being used for money laundering or terrorist financing must therefore always be rejected, without prejudice to the other obligations explained below.

The MB must 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 institutions. The focus is on a risk-oriented approach. The systems and measures must take into account the individual size, organisation and risk situation.

The internal security measures essentially consist of **customer-related due diligence and organisational due diligence**:

2. Internal safeguards - customer due diligence

Customer due diligence is divided into general due diligence **(CDD)**, enhanced customer due diligence **(ECDD)** and **simplified customer due diligence (SCDD).**

The concrete scope of the measures applicable in the 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 under.

The **general duties of care** are generally applicable to all contracting parties. The first six points concern duties in the context of or during the establishment of the business, the last two points concern downstream or ongoing duties:

Simplified due diligence may be applied if 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 indications of a potentially lower risk. This must be determined and documented within the framework of a customer risk categorisation, taking into account the circumstances of the individual case.

Insofar as increased risks of money laundering or terrorist financing may exist, the MB shall apply additional **enhanced due diligence obligations** pursuant to section 15 GWG. This shall be determined and documented within the scope of a customer risk categorisation, taking into account the circumstances of the individual case. The list in Annex 2 to Article 15 (2) GWG specifies factors and possible indications of a potentially higher risk.

2.1 Customer risk categorisation

With the exception of the duty of identification, the general due diligence obligations are to be carried out in a risk-oriented manner. The risk-oriented approach runs through 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. They are classified in one of three risk categories: **, "low", "medium" or "high".**

2.2Identification of natural persons and legal entities

Natural persons are to be identified by means of a valid official identification document containing a photograph of the holder and which fulfils the passport and identification obligation within the country, in particular by means of a passport, identity card or passport or identity card substitute recognised or approved within the country or in accordance with the provisions of the law on aliens. The identity check for **natural Iranian persons is** carried out analogously to the general due diligence obligations, but extended by the enhanced due diligence obligations.

Legal entities or commercial partnerships must be identified by means of an excerpt from the commercial register, an excerpt from a comparable official register or directory, the founding documents or equivalent evidential documents or by inspecting register or directory data. The identification of **legal Iranian persons is** carried out for legal persons analogously to the general due diligence obligations extended by the enhanced due diligence obligations.

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

Identification consists of establishing identity and verifying identity according to qualified documents.

2. 3Clarification to a beneficial owner

The beneficial owner is the natural person,

- in whose ownership or under whose control the contractual partner ultimately stands,
- at whose instigation a transaction is ultimately carried out or a business relationship is ultimately established, or
- which is primarily the beneficiary of an externally beneficial design.

2.4Collecting information about 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 must be obtained and documented as part of the establishment of the business relationship, insofar as this information is not already clear from the business relationship in the individual case.

2.5Origin of funds

The MB must ensure that transactions carried out are also consistent with regard to the available information 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 a mandatory routine control. Only the actually available knowledge about the origin of the assets is to 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, have no obvious economic or legal purpose, or involve a cross-border correspondence relationship with a respondent domiciled in a third country or in a country of the European Economic Area have a risk-increasing effect. In this context, increased due diligence must be applied.

2.7Continuous monitoring and updating obligation

The MB continuously monitors the business relationships including the transactions carried out in the course of these relationships. Continuous monitoring begins with the establishment of the business relationship or with the first use of a service or product. It ends with the termination of the business relationship.

2.8Politically exposed persons

Politically exposed person means 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 whose political importance is comparable. The **FATF** shares this definition of the PEP as a person who is or has been entrusted with a prominent public function and therefore additional AML/CFT safeguards should be applied to business relationships. These measures are preventive and should not be interpreted to mean that all PEPs are involved in criminal activity. 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 State and Government • Government members (national and regional) • Parliamentarians (national and regional)	• Senior military, judicial and law enforcement officials

• Heads of Military, Judiciary, Law Enforcement and Board of Central Banks • Top politicians of political parties	• Senior officials of other state agencies and organs as well as high-ranking officials • 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, city and county assemblies • Senior officials and functionaries of international or supranational organisations

If there are indications that the contracting party is a PEP, **the MLA must be informed before the business relationship is established.** The MLA shall carry out further clarification measures and determine the scope of the due diligence measures resulting from the PEP status (origin of assets, increased, continuous monitoring). Based on his proposals, the management decides on the acceptance or rejection of the business relationship.

2. 9Sanction check

All customers and their beneficial owners are screened against the sanctions lists before a business relationship can be established with MB.

2.10Consequences of failure to comply with due diligence obligations

MB follows a conservative approach with regard to the non-execution termination obligation due to its background and business model. If the customer is not able to fulfil the general due diligence obligations as well as the simplified due diligence obligations or the enhanced due diligence obligations, the business relationship may not be established or continued in accordance with them. Insofar as a business relationship already exists, it shall be terminated by the obligor by way of notice, notwithstanding any other statutory 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, together with the management, decides on the termination or continuation of a business relationship or on the execution of a transaction.

3. Internal safeguards - organisational duties of care

3.1 Money Laundering Officer

The management shall appoint a money laundering officer incl. a central office at management level as well as a deputy. The money laundering officer is responsible for compliance with money laundering regulations. He is directly subordinate to the management. The money laundering officer shall deal with 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 on whether to take the measures is made by the money laundering officer in consultation with the management.

3.3. monitoring and control actions

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

3.4. Continuous monitoring of business relationships

The MB monitors the business relationship, including the transactions, on a continuous basis in order to create a comparison of customer profiles with the respective transaction behaviour in this context. Dynamic monitoring in this context means the appropriate consideration 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 must be monitored, if necessary for a longer period, until the doubts have been dispelled.

3.5 Suspected cases and their reporting

All facts that indicate that an offence under section 261 of the Criminal Code or terrorist financing has been or is being committed or attempted are subject to immediate suspicious activity reporting.

3.6. Regular briefing of employees

The Bank conducts regular training courses to inform and educate staff 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 conducted as WBT. Employees are informed at least once a year about the methods of money laundering and terrorist financing and about the obligations under the German Banking Act (GWG).

3.7. Reliability of employees

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

3.8. Reporting

The money laundering officer shall report to the management at least once a year on the measures taken, the status of implementation of the obligations under the Money Laundering Act, the current risk situation of the institution and significant individual cases.

The Money Laundering Officer shall report on special incidents, significant individual cases or exceptional risks without delay.

3.9. Record-keeping 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.