



# Excerpt of globally applicable Anti-Money Laundering and Anti-Financial Crime Standard



## Anti-Money Laundering Statement

### 1. Introduction

Deutsche Bank (DB) is committed to the highest standards of Anti-Money Laundering (AML) and Anti-Financial Crime (AFC) including Anti-Bribery and Corruption (ABC), Counter Terrorism Financing (CTF), Anti-Fraud and other punishable criminal acts. The members of the Management Board and all employees are required to adhere to these standards to protect DB and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

DB has its headquarters in Frankfurt am Main, Germany and is supervised by the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin).

The Federal Republic of Germany is a member country of the Financial Action Task Force (FATF) and the European Union (EU) and has enacted laws and rules designed to implement the anti-money laundering policies of both FATF and the EU. The goal of these laws is to detect and prevent money laundering and potential terrorist financing.

DB will adhere to all applicable laws and regulations in all countries where it conducts business, or has business relationships to.

DB will examine its AML and AFC strategies, goals and objectives on an ongoing basis and maintain an effective program for the Bank's business that reflects the best practices for a diversified, global financial services provider.

The program is formulated and directed by the Global Head of AFC and addresses all AML-related topics, especially Know Your Customer (KYC), ABC, Sanctions & Embargoes and Anti-Fraud.

For all these topics DB has implemented clear rules and regulations which must be complied with by all DB staff globally.

### 2. Governance Framework

The Global Head of AFC has been tasked by the Management Board on the basis of sec. 25h no. 4 of the German Banking Act with a group wide discretionary power over AML and Financial Crime related matters. He/she has unrestricted access to all information, data, records and systems in the Bank he/she deems necessary to fulfil his/her function.

The Global Head of AFC reports directly to the responsible member of the Management Board.

He/she is responsible for group-wide adherence to applicable AML and Financial Crime regulations and obligations derived from the German AML Act (GwG) and German Banking Act (KWG). In addition, he/she is responsible for establishing and maintaining DB's AML program to identify, assess, monitor and manage risks related to Money Laundering, terrorist financing and Financial Crime.

### 3. Policies and Procedures

DB has developed a clear set of policies and procedures outlining its general AML standards and principles. Detailed documents ensure that these standards are implemented into day-to-day business.

All policies and policy-related documents are published on a global policy platform so they can be accessed by all staff at any time. They are subject to an annual review cycle to ensure their conformity with AML regulations.



## Anti-Money Laundering Statement

### 4. Prohibited Business Relationships

DB must refuse to open an account/enter into a relationship or has to close an existing account/terminate a relationship, if the Bank cannot form a reasonable belief that it knows the true identity of the client and/or UBOs and/or the nature of business or formal requirements concerning the identification of the client and/or UBOs are not met.

In particular, the Bank will not

- Accept assets that are known or suspected to be the proceeds of criminal activity
- Enter into/maintain business relationships with individuals or entities known or suspected to be a terrorist or a criminal organisation or member of such or listed on sanction lists
- Provide or maintain anonymous accounts, accounts for shell banks or payable-through accounts
- Enter into or maintain relationships where the Client has connections with certain prohibited special risk countries (SRCs) (as defined in the Sanctions Policy).
- Enter into or maintain relationships with clients operating in prohibited industries (as detailed in the CRRM Industry Risk list).

### 5. Research and Filing of Suspicious Activity Reports (SARs)/Suspicious Transaction Reports (STRs)

Suspicious activities must be properly handled and escalated within the respective DB legal entity. Regular AML training ensures that staff are reminded of their duty to timely report any suspicious activity to their respective AML Officer, where allowed under local regulations.

### 6. Management and Controls of AML and AFC Risk

DB has developed and implemented a comprehensive set of measures to identify, manage and control its AML risk. These measures are

- A Group-wide AML / AFC Risk Analysis
- Controls
- A robust and strict KYC program
- Special safeguards for correspondent banking relationships
- A training and awareness program for DB staff
- Processes to ensure staff reliability
- A robust and strict Sanctions & Embargoes program
- A global Anti-Bribery and Corruption (ABC) and Anti-Fraud program

#### 6.1. Risk Analysis

DB has implemented an ongoing AML/AFC Risk Analysis to assess the level of risk exposure considering the nature and scope of the DB Group Entity or branch's business activities including clients, products and services, transactions, delivery channels, organisational structure and geographical locations in which it operates. AML safeguards are derived from the results of the AML Risk Analysis.

#### 6.2. Controls

Adherence to the group-wide AML/AFC program needs to be reviewed regularly to ensure that the Bank's efforts are successful. AML Officers in DB Group are therefore obliged to conduct appropriate



## Anti-Money Laundering Statement

controls. The responsible AML Officer must ensure, by implementing adequate customer- and business related controls, that all applicable AML and AFC requirements are being adhered to and security measures are properly functioning.

A Global Controls Program has been developed and implemented to ensure controls are comparable and on the same level in all countries where DB conducts business.

### 6.3. KYC Program

DB has implemented a strict group-wide KYC program to ensure all kinds of customers (natural or legal persons or legal structures, correspondent banks) are subject to adequate identification, risk rating and monitoring measures. This program has been implemented globally and throughout all business divisions

KYC includes not only knowing the clients and entities the Bank deals with (either as a single transaction or ongoing relationship), or renders services to, but also the Ultimate Beneficial Owners (UBOs), Legal Representatives and Authorised Signatories as appropriate.

The program includes strict identification requirements, name screening procedures and the ongoing monitoring and regular review of all existing business relationships.

Special safeguards are implemented for business relationships with politically exposed persons (PEPs) and clients from countries or industries deemed high risk.

### 6.4. Correspondent Banking

DB has implemented special safeguards and monitoring processes for its correspondent banking business. These safeguards encompass, but are not limited to:

- Obtaining sufficient information on the correspondent to fully understand the nature of its business, its reputation, management and ownership structure and maturity of the bank's regulation and supervision in the respondent's country
- Assessment of the respondent's compliance to regulations and supervision, including assessment of compliance
- Risk-classification of all correspondent banking relationships
- Obtaining senior management approval of the onboarding jurisdiction for establishment of new correspondent banking relationships
- Apply transaction monitoring and embargo filtering on transactions with correspondents

DB will not maintain accounts for shell banks or correspondent banking accounts for banks offering services to shell banks. Correspondent banks have to provide confirmation that they will not provide banking services to or engage in business with shell banks.

### 6.5. Approval of New Products

DB has implemented security measures and processes to prevent new products from being misused for money laundering or terrorism financing, or that new products facilitate anonymity of business relationships or transactions.



## Anti-Money Laundering Statement

### **6.6. Training Program**

DB has implemented a comprehensive AML/AFC training program to ensure that all staff, in particular individuals responsible for transaction processing and/or initiating and/or establishing business relationships, undergo AML awareness training.

Deutsche Bank's training is tailored to the business to ensure that staff are aware of different possible patterns and techniques of money laundering which may occur in their everyday business. Training also covers the general duties arising from applicable external (legal and regulatory), internal requirements and the resulting individual duties which must be adhered to in everyday business as well as typologies to recognise money laundering or financial crime activities.

### **6.7. Reliability of Staff**

DB has implemented processes to ensure that only reliable individuals are employed.

### **6.8. Embargo Program**

Compliance with all applicable embargoes is mandatory within DB Group and for all DB employees globally. All EU embargo regulations and all German embargo regulations are binding for the whole DB Group. U.S. embargoes generally apply to U.S. persons and any entity, regardless of their place of domicile or work or where organised, and any individual causing activity with the U.S., whether from inside or outside the U.S.

The Bank's Embargo program comprises controls on new clients and on existing clients as well as minimum requirements for filtering of transactions against embargo lists before they are executed.

### **6.9. Anti-Bribery and Corruption (ABC) and Anti-Fraud**

DB does not tolerate bribery, or any form of corruption. All DB employees and third parties that act on DB's behalf are strictly prohibited from having any involvement in acts of bribery and corruption.

DB's ABC program involves inter alia staff training, monitoring and testing, special requirements for dealings with public officials, or regulations for gifts, entertainments, donations and business courtesies.

DB has implemented an Anti-Fraud Program to ensure that the Bank is not misused for purposes of or that employees do not commit or contribute to any fraudulent activity.

## **7. Record Retention**

All data obtained according to client identification and AML security measures must be documented.

Records must be kept for a minimum of 5 years, notwithstanding potentially longer retention periods under local civil or commercial law.

## **8. Independent Testing**

Adherence to the requirements of DB's AML program is subject to independent testing by DB's Internal Audit function and the Annual External Year-End Auditor.