Company Policy on Prevention of Money Laundering

September 2024

CONTENT

1. OBJECTIVE

The objective of the company policy on prevention of money laundering ("**Policy**") is to establish a general framework for the implementation of know your customer (KYC) principles and prevention of laundering proceeds of crime throughout the Kässbohrer companies ("**Company**" or "**Kässbohrer**") in order to prevent the laundering of proceeds of crime and to fight against the financing of terrorism.

2. DEFINITIONS

"Customer" means real persons or legal entities who procure or use The Company products or services.

"Compliance Manager" means the Company's independent compliance manager.

"FATF" means the International Financial Action Task Force.

"Financing of Terrorism" means the deliberate provision or collection of funds and other assets, by any means, directly or indirectly, considering the use of such instruments in whole or in part by a terrorist organization or by a terrorist act.

"GwG" means the Law of the Federal Republic of Germany on the Prevention of Money Laundering (Geldwäschegesetz).

"Know Your Customer Principles" means the thorough recognition of a real person or legal entity who first contacted the Company and plays an important role in eliminating the risks associated with the Laundering Proceeds of Crime, financing of terrorism, corruption, fraud, bribery and other illegal activities that the Company may encounter due to these individuals.

"Laundering Proceeds of Crime" is the process of legally demonstrating illicitly generated proceeds as set forth in international regulations such as GwG, MASAK and FATF recommendations. It usually comprises the stages of placement, separation, and integration. First, illegitimate funds in cash form are secretly introduced into a legitimate financial system. Then, in order to ensure that the money moves away from its source, the money is moved within the system through many numbers of accounts so that the traceability of the money is prevented. Finally, the proceeds of crime being disconnected from the illicit source are laundered into the country's financial system through legal procedures.

"Management" The board or managing director whichever is the top decision maker as well as applicable at the Company.

"MASAK" means the Financial Crimes Investigation Board of the Republic of Turkiye.

"Public/Government Official" means a person who is permanently, temporarily or for a definite term involved in the conduct of a public activity by appointment or election.

"Politically Exposed Person" means a person assigned to or entrusted with an important public function. Politically exposed persons include, but will not be limited to the following:[1]

- Government heads, ministers and deputy ministers;
- Members of the Parliament;
- Members of supreme courts, constitutional courts or other high-level judicial organs whose decisions are not subject to further appeal, save for exceptional cases;
- Judges;
- The board members of the central banks;
- Ambassadors;
- High-ranking officers in the army;
- Members of the administrative, management or supervisory bodies of state-owned enterprises or persons assigned in the positions equivalent to these; and
- Family members and close business partners of the persons listed above.

"Risk Manager" means an objective and independent assurance and consultancy person within the Company designed to add value to an organization's operations and to improve its processes.

"Sanctions Lists" means the lists of sanctioned individuals, entities or governments.

"System" means the impartial and independent information system operating as integrated with the Company ERP software and analyzing according to the existing international Sanctions Lists, decisions and news in accordance with the requirements of the Know Your Customer Principles.

"Supplier" means real person or legal entity providing goods and services to the Company. These real persons/legal entities are part of the business supply chain and can constitute a large part of the value involved in the Company's products.

"Third Party" means any real person or legal entity acting on behalf of the Company or associated with the Company, such as any distributor, dealer, intermediary, consultant, representative, contractor or subcontractor.

3. SCOPE

The Company is committed to the high standards accepted in the world in the prevention of Laundering Proceeds of Crime. All Third Parties, employees and managers shall be obliged to comply with these standards and be responsible for the implementation of this Policy in

[1] https://www.fatf-gafi.org/documents/documents/peps-r12-r22.html

order to prevent the use of the Company's trademark as well as the products and services for the purpose of Laundering Proceeds of Crime or financing of terrorism.

This Policy has been established taking as the basis, however, is not limited to the regulations and standards listed below and the standards with global practices have also been inspected:

- GwG;
- Basel Principles Declaration on the Prevention of the Use of the Banking System for Money Laundering Purposes[2];
- Financial Action Task Force (FATF) 40 Recommendations[3];
- Wolfsberg Standards[4]; and
- MASAK legislation[5].

4. GENERAL PRINCIPLES

To the extent reasonable and feasible, the Company regularly and continuously supervises its activities against international practices, regulations and conventions related to prevention of Laundering Proceeds of Crime and updates its Policy accordingly. In this context, the Company has determined this Policy. The Company, by establishing an appropriate framework for the Laundering Proceeds of Crime, aims to minimize the possibility of exposure to various risks for both the Company and its employees, including but not limited to:

- ***Reputation Risk.*** Loss arising from significant influence on the Company's reputation. Loss of reputation can lead to damage to the good reputation created by the Company as the result of its activities complying with local and international legislation with all its employees and stakeholders since it has been established and therefore to cause moral and subsequent financial damage to be suffered by the Company.

- *Compliance Risk.* Loss resulting from non-compliance with local and international legislation. Risk of compliance may result in the Company and/or employees to face sanctions such as direct fines, suspension of operations, imprisonment of employees and managers as well as inclusion in sanctions lists.
- *Financial Risk.* Material damage resulting from any of the above risks or a combination thereof and causing adverse financial impact on the Company.

---

[2] https://www.hmb.gov.tr/aklama-sucu-uluslararasi-mevzuat
[3] https://ms.hmb.gov.tr/uploads/2019/01/FATF-Tavsiyeleri-2012.pdf
[4] https://ms.hmb.gov.tr/uploads/2019/01/1-1.pdf
[5] https://www.hmb.gov.tr/aklama-sucu-ulusal-mevzuat

The Company and its employees as well as third parties associated with the Company, are expected to immediately inform the Compliance Manager and/or Risk Manager in written form (e-mail) if they have information about or doubt that they are involved in any relationship related to the Laundering Proceeds of Crime.

A Company employee is expected not to violate this Policy under any circumstances. The Company shall have zero tolerance for the violations of the Policy. Any employee detected to be in breach of this Policy shall be subject to various sanctions, including termination of employment.

In case this Policy has been violated by third parties, the existing contracts must be forthwith terminated, and the necessary legal notifications must be served.

In cases where Third Parties, particularly our employees, have doubts about the compliance of any activity with this Policy, they are expected to notify such suspicions to the Company anonymously or by sharing their personal information at the address https://kaessbohrer.com/en/kaessbohrer-compliance-helpline.

For detailed information on this subject, please review the Company Policy on Whistleblower Protection.

5. IMPLEMENTATION OF THE POLICY

The Company is strongly committed to business ethics and compliance standards. The Company implements globally accepted standards in each geography where it operates and conducts regular checks in order to reduce the risks related to Laundering Proceeds of Crime.

5.1 Due Diligence Study

The principles of recognizing Third Parties that we also work with, such as our business partners and Customers, constitute a very critical process in the assessment of Third-Party risks and are also inevitable to comply with relevant local and international regulations.

The Third-Party acceptance process consists of research processes including but not limited to steps such as (i) identification, (ii) subject of activity, (iii) objective of the transaction, (iv) asset source, (v)

business history, (vi) geography where the operations are carried out, and (vii) reputation research.

Third Parties should be investigated according to the steps above and a due diligence study should be conducted on them. This due diligence study is of utmost importance to keep the Company away from Third Parties involved in illicit activities such as Laundering Proceeds of Crime. In this context, it is required to ensure that Third Party investigations and all information and documents received in this regard are correctly provided during the acceptance process.

There are some points to be considered, before establishing a business relationship with Third Parties, including personnel recruitment processes. Particularly, the situations including but not limited to the following, require more attention and a more comprehensive review.

- Business lines and countries of business;
- Financial position and reputation;
- Historical checks;
- Ethics and compliance policies;
- Persons and institutions[6] operating in high-risk geographies[7];
- Politically exposed persons;
- Persons and institutions that use or desire to use cash in hand transactions;
- Persons and institutions refraining from providing information and documents;
- Persons about whom negative news has been published in the press[8];
- Persons and institutions deemed as suspicious in international lists.

The due diligence study to be performed will be carried out directly by the System by entering the necessary information.

5.1.1. Third Party Recognition

The due diligence study will be started by providing the commercial title and other documents (such as trade registration, tax return) for Third Party legal entities and the complete first and last name on the identity document of Third-Party real persons. This information and documents, if any, to be obtained from the Third Party will be entered into the System without delay and the first step of the due diligence study will be carried out directly by the System.

5.1.2. Third Party Control

The following, namely;

- Negative news;

[6] http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
[7]It is the responsibility of the Risk Manager to check the up-to-dateness of high-risk countries. [8]The results obtained as the result of a simple search on search engines such as Google and Yandex are examined.

- Politically Exposed Persons;
- Suspicious lists; and
- Geography of operations

will be scanned by the System and the result will be automatically filed therein.

In cases where there is no warning is displayed in the System, the decision to conclude a contract shall be assumed by the department that will work directly with the relevant Third Party (such as Human Resources while concluding the employment contract, Sales Department while concluding the sales contract with the customers).

If a warning is displayed in the System, the System will immediately send information in written form (risk@kaessbohrer.com) to the Risk Manager. In this case, upon the request of the Risk Manager, the department that is in direct contact with the Third Party shall also be obliged to immediately forward all information and documents to the Risk Manager.

The Risk Manager will remove the warning from the System if it reviews all relevant information and documents and concludes that there is no violation of the legislation, global standards and/or this Policy. However, if otherwise, it will obtain a legal opinion if deemed necessary and submit its evaluation to the approval of the manager/s together with the proposed administrative review periods. In such cases, the decision to conclude a contract with the relevant Third Party shall only be made by the manager/s.

In the process of acceptance of third parties, if it is determined that the partners or managers of the relevant persons or companies are Politically Exposed Persons, reasonable research will be carried out to detect the source of the assets of the interested parties and a further assessment will be made by the Risk Manager on whether to establish a business relationship with them poses a risk to the Company. As the result of the evaluations made, the final decision on the subject will be resolved by the Management in writing.

All results of the due diligence study on Third Parties, the relevant information and documents must be kept in accordance with the applicable local legislation. The records must be kept for a minimum of eight (8) years, unless otherwise specified in the local legislation, by filing in a clear and comprehensible manner, available for any possible internal and/or external audits.

5.2 Concluding Contracts

Following the due diligence study carried out by the Company to obtain sufficient information about the Third Parties with which it will conduct business, a written contract will be concluded and signed in cases where it is decided to work with such Third Parties.

In order to protect the Company from the risks associated with the Laundering Proceeds of Crime that may be caused by Third Parties, the relevant protective clauses must be added to the contract during the contracting process. In this context, terms and conditions on the right to audit Third Parties, on-site inspection or termination of the contract must be considered. In order to ensure that all contracts

concluded with Third Parties contain the relevant provisions, the approval in written form (e-mail) of the Company's legal counsel, if any, shall be obtained for the signed version of the relevant contract.

5.3 Continuous monitoring

It is not sufficient to check the Third Parties that the Company works with only before the contract signing stage. Third Parties with whom there is an uninterrupted business relationship in accordance with global standards and this Policy must be monitored continuously and regularly, including financial transactions, in accordance with their risk profiles.

As for the Third Parties that are considered to be risk-free during the acceptance process, these real persons or legal entities must be regularly checked by the Risk Manager at least once a year and

(i) whether they are on international sanctions lists, and

(ii) whether there is negative news in the press about them

should be documented.

Subsequent to the warning in the system, the frequency of regular due diligence for Third Parties, who are decided to start or continue to be worked with in accordance with the decision of the Company's manager/s, shall be determined by the Risk Manager according to the extent of the risk, which such frequency will be at least every six (6) months. For such assessments,

(i) Negative news search in the press about the relevant real persons and legal entities, company partners and senior managers;

(ii) International sanctions list scanning;

(iii) Tracking of changes in fields of activity; and

(iv) Tracking of countries where foreign trade operations are carried out

will be performed by the system by means of researching the public resources. The research in this context will be carried out by the Risk Manager.

As the result of this research, the decision to continue working in the event of the emergence of a new risk that did not exist before will be made only by the Company's manager/s, if necessary, by obtaining a legal opinion. The decision of the Company's manager/s will be added to the opinion of the Risk Manager and legal, if any, for archival purposes.

In cases where it is deemed that no new risk element has been formed, the due diligence study will continue to be performed at the frequency determined by the Risk Manager.

5.4 Third Party Requests

Various institutions may request documents and information regarding their transactions with the Company or Third Parties. If any Company employee is the addressee of such a request, he/she must share this request with the Risk Manager without delay. The responses to such requests should be subject to the approval of the Risk Manager without exception and should not contain any inaccurate/incomplete information. Furthermore, all internal and external correspondence related to this request process, if any, must be recorded in physical and in any case in electronic form and stored.

5.5 Training

In order to ensure compliance with local and international regulations regarding the Laundering Proceeds of Crime and to raise awareness of the risks associated with the relevant policies and rules of the institution, all relevant employees should receive regular trainings.

All Company employees will be required to receive training on prevention of Laundering Proceeds of Crime at the time of employment and to attend this training at least once a year. Furthermore, the Company may, if it deems necessary, provide awareness-raising trainings on prevention of Laundering Proceeds of Crime arrangements or request that employees receive training from other sources on these issues at its own expense. The organization and follow-up of the trainings will be carried out by the Company Human Resources Department together with the Risk Manager.

5.6 Audit

External auditors will conduct a general audit on the activities on Prevention of Laundering Proceeds of Crime in the Company at least once a year and/or upon the request of the Management and report the audit results to the manager/s.

6. AUTHORITIES AND RESPONSIBILITIES

Updating this Policy is the responsibility of the Risk Manager.

Company employees and managers shall be obliged to comply with this Policy, and Company business partners are expected to comply with this Policy to the extent possible. If there is a difference between this Policy and the local legislation in force in the countries where the Company operates, the more restrictive one shall prevail.

In the case Company employees witness a transaction that is contrary to this Policy, the applicable legislation or the Company's Code of Conduct in accordance with the above-mentioned articles, they will personally be required to notify the suspicion of violation over the address https://kaessbohrer.com/en/kaessbohrer-compliance-helpline.

Employees may also address questions to the Management, Risk Manager and/or Compliance Manager at any time regarding sanctions and export control and the implementation of this Policy.

The Risk Manager is responsible for conducting audits that increase the likelihood of detection of possible violations and ensuring that risk-mitigating controls related to the identified risks are implemented throughout the Company.

As mentioned in more detail above, in the event of a breach of this Policy, criminal sanctions may be imposed, including dismissal of employees and termination of the contract concluded with Third Parties.

7. REVISION HISTORY

This Policy entered into force on 15 February 2023.

Revision	Date	Remarks
No.1	September 2024	Updates were made due to the new whistleblower system as stipulated in the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.