AAK Group Anti-Money Laundering Policy

8 May 2026

Contents

1. Introduction and scope

AAK AB (publ) ("AAK") is committed to responsible business practices when it comes to avoid being complicit in and counteract money laundering practices. This Anti-Money Laundering Policy (this "Policy") sets out general guidance and principles on how we should prevent and detect money laundering (including financing of terrorism) with the purpose of raising awareness of such issues among all employees within AAK. This Policy highlights the importance of AAK assessing risks of money laundering in every business relationship and transaction. The aim of this Policy is to prevent or mitigate risks that AAK is involved in illicit behaviour connected to money laundering in breach of legal obligations and statements made in AAK's Code of Conduct.

This Policy is applicable to all employees and directors of AAK and all its subsidiaries, including temporary employees, contract employees and agency personnel who work at AAK premises or under the direction of AAK (all collectively referred to as "employees").

2. Responsibility, failure to comply and no retaliation

It is the responsibility of the respective ExCom member to ensure that this Policy is implemented as required and that business is conducted in compliance with this Policy. The function with overall responsibility for this Policy is Group Legal and Compliance, who will report the results of this review process to the Chief Financial Officer.

Notwithstanding the above, each employee is responsible to observe and promote this Policy. Failure by employees to comply with this Policy may lead to disciplinary action, including termination of employment and it may also lead to liability in damages and criminal charges.

No employee shall be retaliated against for acting in good faith in accordance with this Policy.

3. Training

AAK will, from time to time, provide training to relevant employees regarding this Policy.

Group Legal and Compliance shall determine the content of the training and the relevant employees who will be required to complete the training.

4. Anti-money laundering and financing of terrorism

4.1 What is money laundering?

"Money laundering" is the term used to describe the process of making proceeds of a criminal activity to appear to have come from a legitimate source and, thus, concealing its true origin. Money laundering is illegal because it enables criminals to profit from crime.

Money laundering often involves a chain of transfers to foreign banks and legitimate businesses and multiple transfers, which makes it difficult to detect. Anyone accepting payment for services and products is vulnerable to abuse by money launderers.

In general, money laundering typically involves the following three steps:

- Placement: Money derived from illicit activities is placed into the financial system. This may be done by, for example, breaking up sums of cash into smaller amounts that are later deposited at different locations, repaying loans or concealing it in legitimate businesses in which cash handling is part of the day-to-day business.

- Layering: Once the money is in the financial system, it is moved in order to conceal its true origin (often several times). This may be done by conducting complex international transactions involving offshore company structures.

- Integration: In order for the individuals or groups that initiated the money laundering process to enjoy the illegal profit, the money must be reinvested in a manner that appears legitimate. This may be done by, for example, investing the money in legitimate businesses or by purchasing properties.

“Financing of terrorism” is closely aligned with the concept of money laundering and entails that terrorism is supported by direct or indirect contributions or by gathering, receiving or transferring money or other assets that serve the purpose of financing terrorism. For the purposes of this Policy, “financing of terrorism” is included in the term “money laundering”.

4.2 How could AAK become complicit in money laundering?

Primarily, AAK may become complicit in money laundering schemes at the integration stage, where AAK may be used for money laundering through schemes involving our normal trade transactions and where value transfers disguise or legitimize the illicit origins of the funds.

Being complicit in money laundering, where the money laundering purpose is known but also in circumstances where measures can be assumed to be taken for the purpose of money laundering, can lead to criminal liability for individuals and, in some jurisdictions, for companies. It may also lead to severe fines and reputational damage.

4.3 Means to combat money laundering

The principal way in which AAK may be used for money laundering is through schemes involving our normal counterparty trade transactions, where value transfers disguise or legitimise the illicit origins of the funds. Counterparties are all parties with which AAK has a direct business relationship, e.g. agents, suppliers, distributors and customers. A counterparty can be e.g. an individual, a company, an organisation or a public authority.

Examples of procedures which are frequently used by money launderers are:

- Incorrect invoicing (over- or under-)

- Receipt of third party payments (i.e. payments from other party than approved counterparty)
- Requests for credits to be paid to a third party (i.e. returns, discounts or other payments made by the company to a party other than the approved counterparty)
- Requests for delivery to other party than the approved counterparty
- Requests for invoicing to other party than the approved counterparty
- The order is negotiated and agreed with a party other than the approved counterparty

In order to avoid money laundering, AAK shall be able to demonstrate that internal anti-money laundering routines have been implemented. Such internal routines will demonstrate diligent conduct and that AAK does not have any reasons to suspect that money derives from criminal activities.

Due-diligence investigations shall be conducted in proportion to the level of risk posed by a specific relationship. This means that some parties require more in-depth investigation than others. Certain transactions should be refrained from completely. AAK shall not establish or maintain a business relationship or carry out any occasional transactions if we do not have sufficient information about the business partner.

4.3.1 Know your counterparty

Financial transactions are an essential part of our relationships with suppliers, employees, customers and financial counterparties in our day-to-day business. In order not to be complicit in any form of money laundering through such financial transactions, AAK must carefully assess whether our products and services can be used for money laundering purposes. AAK must always act diligently and have knowledge of when suspicion should be raised (see below Section 4.3.3 for a non-exhaustive enumeration of “Red Flags”).

AAK shall not establish or maintain a business relationship or carry out any occasional transactions if we do not have sufficient information about the counterparty. There shall be internal controls and standard practices to identify and to verify counterparties and also business contacts of occasional nature. Counterparty checks may also include other business controls. As a minimum, the following information shall be collected to assess risks connected to third parties:

- Name of the company, registered address, country of origin/incorporation and ID/registration number
- The business sector that the company operates in
- Owner(s) of the company (ultimate beneficial owner and major shareholders)
- Intermediaries involved and the reason(s) for involving them (if any)
- Bank(s) used by the counterparty

Note that additional information gathering activities may need to be conducted to exclude unwanted third party compliance risks.

As a minimum, information collected needs to be retained for a period of one year from the end of the relationship with the counterparty as well as retaining any suspicious activity reports for the same amount of time unless local law requires longer retention periods. Each relevant AAK entity is responsible for saving a copy of the documentation.

4.3.2 Transaction monitoring

Apart from conducting counterparty checks in relation to our counterparties as referenced in Section 4.3.1, AAK must ensure that we continuously monitor our business relationships and occasional financial transactions in order to detect activities and transactions that deviate from what can be expected in light of our information about the counterparty and our products and services. The level of monitoring should be decided based on the result of the counterparty check and on deviating activities in relation to the transaction.

4.3.3 Red Flags

There are certain circumstances in business that provide indications of risks that a potential counterparty may try to use AAK for money laundering activities, so-called “Red Flags”. Below are some examples of typical Red Flags to remain watchful for. Note, however, that these are only a few examples of potential money laundering risks, and that any suspicion in regards to a counterparty or transaction should be reported to Group Legal and Compliance.

- The requested information is incomplete and inconsistent and it is difficult to find information about the counterparty in open sources.
- The counterparty’s ownership structure appears to be unknown, unusual or too complicated for its business.
- The counterparty is established in or has other connections to/in high-risk countries.
- The stated contact information (e.g. phone, number, e-mail, address) seems to be directed to a third party.
- The counterparty seems to be a shell company or a letter box company (a company without any physical presence or a clear business purpose).
- The counterparty has no website or the website does not appear relevant to the business stated.
- The counterparty is suggesting to use intermediaries for no good reason or the transactions otherwise seems complicated (e.g. involves many different parties) for no good reason.
- The counterparty, its directors, or beneficial owner is a PEP (politically exposed person) or a family member or known colleague of a PEP.

- The counterparty requests that the payment to be made by or to a third party (including parties stated to be associated with the business partner) or by the use of, or to, bank accounts in different countries without no good reason.

- The counterparty requests products to be delivered to, or payments or repayments to be made to, a third party (including parties stated to be associated with the business partner).

- The counterparty uses bank accounts in several countries without good reason.

- The payment for goods or services follows another route than the products or services (e.g. via another country or via another legal entity), in particular if the payment is made from a tax haven.

- The counterparty makes an unusually large order which does not seem to be consistent with the counterparty's business or the products ordered seem to be irrelevant for the counterparty's stated business activities and/or the counterparty seems unfamiliar with the ordered products, its performance or other characteristics.

5. Raise concern

Compliance with this policy is mandatory for all employees of AAK. It is vital that everyone knows the rules and complies with them. You are encouraged to raise questions and concerns at the earliest possible stage about;

(i) The scope and application of this policy; and

(ii) any instance or suspicion of malpractice or any action which may be a breach of this policy.

Such concerns will be treated in the utmost confidence and should be raised with Group Legal and Compliance or via the WhistleB toolhttps://report.whistleb.com/aak . No employee shall be retaliated against for acting in good faith in accordance with this policy.

Penalties for violations of anti-money laundering laws can include fines and imprisonment, and settlements with authorities can amount to hundreds of millions of euros or dollars. If you are uncertain on how to act in a specific situation, you should consult with Group Legal and Compliance. If you suspect that AAK or anyone acting on AAK's behalf is acting in violation of this Policy, you are required to report such suspected misconduct.

6. Review

This policy is reviewed annually by the Audit Committee.

Making *Better* Happen™

AAK