Fiskars Group Anti Money Laundering Policy

Version history

Person responsible			Kaisa Vuorinen				
Owner			Fiskars Corporation, Group Treasury				
Framework code	1.B.		**Next revision date**				
Version	**Date**	**Author**	**Description**	**Reviewed**		**Approved**	
				Date	**By**	**Date**	**By**
1.0	30.11.2022	Kaisa Vuorinen		31.3.2023 11.1.2023	CFO Jussi Siitonen, Legal & Compliance	20.4.2023	FGLT
2.0	30.8.2024	Kaisa Vuorinen	Update to 8, 9.1. and 9.2.5	6.9.2024	CFO Jussi Siitonen, Legal & Compliance	18.9.2024	FGLT

Fiskars Group
Fiskars Oyj Abp
Keilaniementie 10
P.O. Box 91
FI-02151 Espoo
Finland
www.fiskarsgroup.com

Table of contents

1 Purpose and scope

Fiskars Anti Money Laundering Policy[1] (Policy) describes the processes to be followed and measures to be taken to ensure compliance with relevant legislation, regulations and guidelines aimed at preventing money laundering and terrorist financing. Failure to comply with the Policy may lead to investigations, fines, reputational damage, cancellation of existing financing facilities, exclusion from services of financial intermediaries and denied access to financial markets.

The Policy applies to all Fiskars Group companies (Group companies), officers and employees. It also applies to all persons engaged to perform work for Fiskars Group, including temporary agency personnel, contractor personnel and non-employee agents on its behalf (referred to as employees) and all transactions carried out in the name of or on behalf of Fiskars. Any deviations and exemptions from the Policy shall be applied for from the Finance Function, the Group Treasury and Risk Management.

The Policy applies in all countries in which Fiskars Group does business. This includes countries through which shipments or financial transactions flow. It shall be noted that breach by any Fiskars Group company, officer or employee may lead to consequences for any other or all Fiskars Group companies.

2 Ownership, review and approval

This Policy is owned by Finance Function, the Group Treasury and Risk Management (Treasury). The Policy is reviewed yearly and minor updates are approved by the Chief Financial Officer (CFO). Any material amendments and updates to the Policy are approved by the Fiskars Group Leadership Team (FGLT).

3 Communication

The Treasury is responsible for communicating this Policy, and for providing advice regarding the implementation of the Policy. In questions pertaining to specific legislation, regulations and guidelines the Legal and Compliance provides assistance.

4 Document’s location in the policies and instructions framework

This document belongs to the group of Group policies, Finance 1.B.

[1] This document is based on International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations – Adopted by the FATF Plenary in February 2012, Updated March 2022

5 Validity

This document is valid as of 1st May 2023.

6 Responsibilities

The Treasury maintains the Policy documents, and makes necessary updates.

Legal and Compliance function is responsible for providing assistance in questions pertaining to legislation, regulations and guidelines issued by relevant authorities.

Legal entity controller in each legal company is responsible for implementing the necessary processes and controls to enable compliance with the Policy. The legal entity controller is responsible for ensuring compliance with the Policy as well as with any other relevant legislation, regulations and guidelines.

Before engaging in any transaction, any officer or employee of Fiskars Group must be certain, that the contemplated transaction is permissible under relevant legislation, regulations and guidelines. In unclear circumstances the Legal and Compliance function needs to be involved at the outset and provide prior approval before the transaction can proceed.

7 Legislative background and international recommendations

1) Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing; Regulation (EU) 2015/847 on information on the payer accompanying transfers of funds; 5th anti-money laundering directive (Directive (EU) 2018/843)

2) The FATF recommendations

International standards on combating money laundering and the financing of terrorism and proliferation have been issued by Financial Action Task Force (FATF), an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

The FATF recommendations relied upon for the purposes of this document were adopted by the FATF plenary in February 2012 and updated in March 2022.

8 Risk assessment - risk based approach[2]

Prior to entering into any transaction a risk assessment to evaluate the risks of money laundering and financing of terrorism need to be made. In conducting the risk assessment the nature, size and extent of the activity shall be taken into account.

There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced counterparty due diligence measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of counterparties, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher risk situations include the following:

1) Counterparty risk factors:
    a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution from where/to which the payments from/to the counterparty are made, and the counterparty).
    b) Non-resident customers
    c) Legal persons or arrangements that are personal asset-holding vehicles
    d) Companies that have nominee shareholders or shares in bearer form
    e) Businesses that are cash-intensive
    f) The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.
2) Country or geographic risk factors:
    a) Countries identified by credible sources as not having adequate AML/CFT systems
    b) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations
    c) Countries identified by credible sources as having significant levels of corruption or other criminal activity
    d) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country
    e) Countries listed on the Indicative, non-exhaustive list of conflict-affected and high-risk areas (CAHRAs) under regulation (EU) 2017/821
3) Product, service, transaction or delivery channel risk factors:
    a) Private banking
    b) Anonymous transactions (which may include cash)

[2] FATF (2012-2022), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France; p.68-69

c) Non-face-to-face business relationships or transactions

d) Payment received from unknown or un-associated third parties

Examples of potentially lower risk situations include the following:

1) Counterparty risk factors:
   a) Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership
   b) Public administrations or enterprises
2) Country risk factors:
   a) Countries identified by credible sources as having effective AML/CFT systems
   b) Countries identified by credible sources as having a low level of corruption or other criminal activity

9 Preventive measures

Prior to entering into any transaction or agreement of any significant value, Fiskars officer or employee is required to identify and verify the identity of the counterparty, and understand the nature of its business, its ownership and control structure.

9.1 Counterparty due diligence and record-keeping[3]

Counterparty due diligence (CDD) measures shall be undertaken when:

1) establishing business relations;
2) carrying out occasional transactions above the threshold of USD or EUR 10.000 equivalent
3) there is a suspicion of money laundering or terrorist financing; or
4) there are doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD measures to be taken are as follows:

1) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. The type of information that would normally be needed to perform this function would be:
   a) Name, legal form and proof of existence – verification could be

[3] FATF (2012-2022), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France; p.14-15, 65-66

obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

b) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company).

c) The address of the registered office, and, if different, a principal place of business.

2) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner. For legal persons and arrangements this should include understanding the ownership and control structure of the customer.

a) For legal persons:

(1) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person; and

(2) to the extent that there is doubt under (1) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(3) Where no natural person is identified under (1) or (2) above, reasonable measures to identify and to verify the identity of the relevant natural person who holds the position of senior managing official should be taken.

b) For legal arrangements:

(1) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

c) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

3) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

4) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Fiskars' or its officers' or employees' knowledge of the customer, their business and risk profile, including, where necessary, the source of funds

Each of the above CDD measures (1-4) shall be applied, but the extent of such

measures shall be determined based on risk based approach.

The above shall also apply to existing customers on the basis of materiality and risk. If the customer due diligence measures laid down above cannot be carried out, a customer relationship cannot be established, a transaction concluded or a business relationship maintained.

Where the counterparty or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

The counterparty due diligence measures set out above do not have to be repeated every time a transaction is conducted with the counterparty. The Group company or Fiskars officer or employee is entitled to rely on the identification and verification steps already undertaken, unless there are doubts about the veracity of that information. Examples of situations that might lead to having such doubts could be where there is a suspicion of money laundering in relation to that counterparty, or where there is a material change in the way that the counterparty's account is operated, which is not consistent with the counterparty's business profile.

The documents, data and information collected under the counterparty due diligence process shall be kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of counterparties. The CDD information and records should be available to domestic competent authorities upon appropriate authority. The records shall be maintained for at least five years or as long as national legislation or regulation requires, whichever is longer.

9.2 Additional measures for specific counterparties and activities [4]

9.2.1 Politically exposed persons

In relation to foreign politically exposed persons (PEPs) (whether as counterparty or beneficial owner), the Group companies are required, in addition to performing normal customer due diligence measures, to:

1) have appropriate risk management systems to determine whether the customer or the beneficial owner is a politically exposed person;
2) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
3) take reasonable measures to establish the source of wealth and source of funds; and
4) conduct enhanced ongoing monitoring of the business relationship.

Group companies are required to take reasonable measures to determine

[4] FATF (2012-2022), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France; p.16-17

whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, Group companies are required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs

9.2.1.1 Definition of politically exposed person[5]

PEP stands for a natural person who is, or who has been, entrusted with prominent public functions:

1) heads of a state, heads of government, ministers and deputy or assistant ministers;
2) members of parliament or of similar legislative bodies;
3) members of the board of directors of political parties;
4) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; members of courts of auditors or of the boards of central banks;
5) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
6) directors, deputy directors and members of the board or equivalent function of an international organization (such as UN, organizations associated with UN, Council of Europe, NATO and WTO); and
7) members of the administrative, management or supervisory bodies of an enterprise which is wholly (100 %) state-owned. A relative or close associate ("RCA") to a PEP shall also be treated as PEP(s). A relative stands for:
8) a spouse, or a person considered to be equivalent to a spouse, of a PEP;
9) children of a PEP and their spouses, or persons considered to be equivalent to a spouse; and
10) the parents of a PEP, or the extended meaning as defined in local legislation.

Brothers and sisters, grandparents/grandchildren are not relatives according to this definition.

9.2.2 Money or value transfer services

Group companies should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

[5] As generally defined by financial institutions

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or listed by the MVTS provider as its agent.

9.2.3 New technologies

Group companies should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies. In the case of Group companies, such a risk assessment should take place prior to the launch of the new business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

9.2.4 Wire transfers

Group companies should ensure that counterparties include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. Group companies should ensure that the recipient of the product and the payer are the same counterparty.

9.2.5 Cash transactions and gift cards

Group companies and retail shops, other than Georg Jensen retail shops, may not accept cash payments exceeding USD or EUR 1.500 equivalent in a single payment or series of payment transactions that are made by or appear to be made by the same paying party within a short period of time. Gift cards may not be issued against cash payments in excess of USD or EUR 1.500 equivalent.

Returns shall be refunded using the same payment method that was used to pay for the original purchase.

With regards to Georg Jensen stores, the maximum limit for cash payments set by the local authorities shall be observed. Records shall be maintained of all single or apparently linked cash (or cash-like) transactions equal to or exceeding USD or EUR 10.000 equivalent, or the threshold defined by applicable law (whichever is lower). The records shall be maintained for either a minimum of five years or as long as required by the national legislation or regulation, whichever is longer. Records are considered adequate if the following can be demonstrated:

- A procedure for monitoring cash or cash-like transactions
- Records of cash or cash-like transactions, including databases, financial system reports, invoices
- Records of your reporting cash transaction breaches to the relevant authority, including letters or emails

Where required by law, such transactions shall be reported to the relevant designated authority.

Payments related to payroll and incentive payments are excluded from the measures described in chapter 9 of this Policy.

10 Suspicious transactions

If a Group company suspects or has reasonable grounds to suspect that funds involved in dealings with the Group company are the proceeds of a criminal activity or are related to terrorist financing, it shall contact the Legal and Compliance function without delay. All suspicious transactions regardless of amount shall be reported.

11 Contacts

VP, Group Treasury and Risk Management, Kaisa Vuorinen,
kaisa.vuorinen@fiskars.com, +358 50 327 9095

compliance@fiskars.com