POLICY ON PREVENTIVE MEASURES AGAINST MONEY LAUNDERING AND TERRORISM FINANCING

CRESCO CAPITAL SERVICES A/S

Reviewed and updated in 2024

CONTENT

1 Introduction

Cresco Capital Services A/S (hereinafter "CCS") is a registered Alternative Investment Fund Manager (hereinafter AIFM) with the Danish Financial Supervisory Authority. This policy applies to all representatives, including employees, management, and owners of CCS.

According to the Danish Act on Measures to Prevent Money Laundering and Financing of Terrorism[1] (hereinafter the "AML Act"), companies covered by the act must have sufficient written policies, procedures, and controls to effectively prevent, mitigate, and manage the risks of money laundering and terrorist financing. According to section 1, clause 1, no. 9 of the AMl Act, AIFMs with direct customer contact, such as CCS, are subject to the AML Act.

The purpose of this policy is to meet the requirements to a written policy, as well as to ensure that employees and the management in CCS can fulfill the requirements of the AML Act. The policy is thus a comprehensive document containing both policy and risk management strategy, procedures, and controls.

[1] Bekendtgørelse af lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven). LBK nr 807 af 21/06/2024

2 Definition of Money Laundering and Terrorist Financing

The purpose of the AML Act is to prevent money laundering and terrorist financing. A crucial part of this purpose is that persons or companies covered by the act are subject to a reporting obligation in cases of suspicion that cannot be dismissed.

In the AML Act, money laundering is defined as follows:

- Illegally receiving or acquiring economic proceeds or funds obtained through a criminal offense.
- Illegally concealing, storing, transporting, assisting in the disposal of, or otherwise securing the economic proceeds or funds from a criminal offense.
- Attempting or assisting in such actions.

Money laundering also includes actions carried out by the person who committed the criminal offense from which the proceeds or funds derive. There is no de minimis threshold for when an action is covered by the definition of money laundering.

Money laundering transactions can take various forms, aiming to change the identity or nature of criminal proceeds so that they later appear as legitimate funds or assets.

Money laundering typically occurs in different stages:

- Placement: The physical placement of proceeds – depositing into the financial system.
- Layering: Separating the proceeds from their source through (financial) transactions to obscure the audit trail and achieve anonymity.
- Integration: Reintroducing the funds into the economic sphere in a form where the proceeds are converted into assets that appear legitimate.

The primary obligations for CCS' employees and management to counteract money laundering and terrorist financing mainly involve:

- Identifying customers with proper identification when a business relationship is established.
- Updating the customer information.
- Investigating circumstances that are suspicious or appear suspicious.
- Reporting any suspicion of money laundering and/or terrorist financing in accordance with this policy.

Terrorist financing is understood as financing terrorism as defined in section 114b of the Danish Penal Code concerning actions covered by sections 114 and 114a of the Penal Code.

3 Risk Assessment

The AML Act requires CCS to identify and assess the risk that the company may be misused for money laundering or terrorist financing. The risk assessment must be based on CCS's business model

3.1 CCS' Business Operations

CCS's business model includes managing alternative investment funds (hereinafter AIFs) that primarily invest in forestry properties in Europe. CCS typically assists AIFs with (i) purchasing forestry properties, including determining market/offer values, (ii) obtaining mandatory information about the property, (iii) contacting local forest managers, and (iv) selling properties.

CCS does not receive cash. The funds that typically move through CCS's accounts are electronic payments for disbursed expenses, management fees, and fees for completed property transactions. CCS operates in a professional environment where other professional actors, who have independent customer relationships with the client, such as lawyers, accountants, financing banks, or mortgage institutions, are involved in property transactions.

The asset that is the subject of CCS's work is real estate. Thus, it is an asset that cannot be transferred or moved outside the borders of the respective countries. If a real estate asset is used for money laundering or terrorist financing, it becomes a question of whether the funds used in the transaction have or can acquire a connection to money laundering or terrorist financing.

CCS's customers are primarily Danish investors in the form of Danish companies, funds, and individuals.

3.2 Risk of Money Laundering

3.2.1 National Risk Assessment

In the National Risk Assessment for Money Laundering in Denmark 2022[2], AIFMs are not explicitly mentioned as a particularly risky business type. However, real estate transactions are mentioned as a method used to launder the proceeds of crime. In the National Risk Assessment for Money Laundering it is mentioned that on one hand, real estate is an area where one can invest a significant amount of money in an asset that rarely decreases significantly in value. On the other hand, it is difficult to remain anonymous, and both banks and real estate agents investigate the origin of the funds. Therefore, according to the national risk assessment, the risk that real estate transactions are misused for money laundering is *moderate*. The risk assessment mentions that actors may use illegal means to renovate/improve a property for resale.

Manipulation of property valuation can also occur when criminal actors, in connection with real estate transactions, value the property below or above market value to either use (cash) proceeds for the purchase or create a "legal" income through resale, e.g., by agreeing on a lower property value and then

[2]Den Nationale risikovurdering af hvidvask, Hvidvasksekretariatet, 2022: https://anklagemyndigheden.dk/sites/default/files/inline-files/risikovurdering_webtilg%C3%A6ngelig_v1.0_0.pdf

reselling the property at market value (with a profit). It can be challenging to determine whether proceeds from property sales or rentals are a result of market price developments or property improvements carried out with criminal proceeds. Real estate acquired with criminal proceeds can also serve as a means to obtain additional financing options, such as loans and credits, which can help obscure the criminal activity.

3.2.2 Supranational Risk Assessment

The European Commission has published its Supranational Risk Assessment Report of October 27 2022[3], (hereinafter "SNRA"), which assesses the vulnerability to money laundering and terrorist financing in various areas, including investment in real estate. According to the SNRA (annex 1)[4], the level of money laundering and terrorist financing threat related to investment in real estate is considered as very significant (level 4), as the "*real estate sector is not organised well enough to sufficiently raise risk awareness. The involvement of different kinds of obliged entities in a real estate transactions/ business relationships tends to dissuade the sector from conducting its own customer due diligence. Suspicious transaction reporting is not satisfactory. The checks are difficult to carry out and there is not always a sound information trail*" (p. 183). According to the SNRA: "*Common methods used by criminals in ML/TF schemes involve the use of complex loans or credit finance, intermediation via professionals, the use of corporate vehicles, manipulation of the appraisal or valuation of a property, the use of monetary instruments such as cash or cheques, the use of mortgage schemes or the use of properties to conceal money generated by illegal activities. It is also common for criminals to invest high amounts of money (ill-gotten funds) to rebuild or renovate real estates. Afterwards, they could use them for their own benefit (houses, apartments or business offices) or they could sell those real estates with a much higher price than they purchased and justifying the income*" (p. 179).

3.2.3 CCS' Risk Assessment of Money Laundering

CCS assesses that the type of renovation and manipulation of property values described in the National Risk Assessment 2022 and SNRA 2022 in real estate transactions would occur without the involvement of AIFMs, as AIFMs are a relatively costly element and increase the risk of potential money laundering being detected.

Additionally, CCS primarily operates within the EU, and for the vast majority of cases, CCS's business relationships are with Danish companies, funds, or individuals whom CCS has physical contact with during the sale or purchase process.

Based on the above, CCS assesses the risk that CCS directly, through its work, will become involved in or misused for money laundering as low.

Based on the above, CCS assesses that there may be a risk of money laundering in the following situations:

- Real estate transactions where, in CCS's assessment, the property is not sold at market price between buyer and seller.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:554:FIN
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN

- If the property has been improved with funds obtained from money laundering by the seller.
- If the buyer pays for the property with funds derived from money laundering.
- Real estate transactions where the transaction is not completed, and deposited funds by the seller must be paid to the buyer.

These situations will be of particular concern to CCS in terms of the risk of being misused for money laundering. The above is not an exhaustive list of situations that may involve a risk of money laundering.

3.3 Risk of Misuse for Terrorist Financing

Terrorist financing is understood, according to section 114b of the Penal Code, as (i) directly or indirectly providing financial support to, (ii) directly or indirectly procuring or collecting funds for, or (iii) directly or indirectly making money, other assets, or financial or similar services available to a group or organization that commits or intends to commit actions covered by sections 114 or 114a.

Based on CCS's business operations, as described in section 3.1, CCS assesses the risk of directly being misused for the actions described above in letters (i)-(iii), as well as for the reasons mentioned in section 3.2.3, as low.

If suspicion arises that a customer has a connection to terrorism, it will be checked against official terror lists (terror lists) and the EU Sanctions Map. If this is the case, CCS will report to the DFIU according to section 7.2.

3.4 Risk Management

Based on the above, CCS has chosen a risk management strategy where standard information is obtained on all customers at the establishment of a business relationship, and this information is verified by an independent source (e.g., a search in a reliable and independent register or database or a document issued by a public authority). Additionally, as part of the establishment of the business relationship, CCS collects information about the customer's purpose with the investment and where the customer's funds originate from. CCS will increase its awareness if situations involve factors mentioned in Appendix 1a under elevated risk. For example, if the customer's ultimate beneficial owner is not based in Denmark or the EU/EEA, or if the customer cannot adequately account for the origin of the funds or the nature/intention of the business. If CCS suspects that one of the situations mentioned in section 3.2.3 is occurring, CCS will seek to confirm that there is no money laundering involved in the situation. If this cannot be confirmed, a report must be made according to section 7.2.

4 Know-Your-Customer Procedures

4.1 When to Conduct KYC-Procedures?

It is essential that CCS knows its customers. The anti-money laundering rules therefore require CCS to conduct know-your-customer procedures (KYC-procedures) in situations where:

- A business relationship is established.
- A customer's relevant circumstances change, and otherwise at appropriate times.
- A one-time transaction of at least EUR 15,000 is conducted, whether the transaction occurs in one go or as several transactions that are or appear to be connected.
- There is suspicion of money laundering or terrorist financing, regardless of whether the condition in no. 2 is met or not.
- There is doubt as to whether previously obtained information about the customer's identity is correct or sufficient.

For CCS, most situations where KYC-procedures need to be conducted will be those mentioned under nos. 1 and 2.

4.2 Implementation of KYC-Procedures

As part of the implementation of KYC-procedures, CCS must ensure the following:

- The customer's identity information.
    - If the customer is an individual, the identity information must include name and the Danish Civil Registration Number (CPR) or similar if the individual does not have a Danish Civil Registration Number. If the individual does not have a Danish Civil Registration Number or similar, the identity information must include the date of birth.
    - If the customer is a legal entity, the identity information must include name and Danish Business Registration Number (CVR) or similar if the legal entity does not have a Danish Business Registration Number.
- Verification of the customer's identity information based on documents, data, or information obtained from a reliable and independent source.
- Identity information on the beneficial owners and taking reasonable measures to verify the identity of the beneficial owners so that the company or person is certain of who the beneficial owners are. If the customer is a legal entity, reasonable measures must also be taken to determine the legal entity's ownership and control structure.

- Assess and, where relevant, obtain information about the nature and intended purpose of the business relationship.
- Continuously monitor an established business relationship. Transactions conducted as part of a business relationship must be monitored to ensure that the transactions are consistent with the company's or person's knowledge of the customer and the customer's business and risk profile, including, if necessary, the origin of the funds. Documents, data, or information about the customer must be kept up to date.

It must also be checked whether the customer or the beneficial owners are a politically exposed person (PEP) as defined in section 5.1.

The information obtained as part of the KYC-procedures must be stored at CCS in accordance with section 7.3, and it must be clear from the information when it was obtained (in a way that cannot subsequently be changed).

4.2.1 Purpose, Nature, and Origin of the Funds

When CCS assesses the customer's purpose and the intended nature of the specific transaction, CCS must inquire where the customer's funds, used for the acquisition of properties, originate from. The information must be compared with other circumstances, e.g., if the acquisition is financed with a mortgage secured by the property. If the customer's explanation is not sufficient or likely, CCS must determine what additional information, if any, CCS must request to verify the customer's explanation. This could be in the form of financial statements or other wealth information.

4.3 When Does a Business Relationship Exist?

When CCS enters into agreements with new investors, a business relationship is established. In such cases, CCS will obtain the necessary information about the customer in the form of the investors.

One-time Tasks and Assessments

According to the anti-money laundering rules, it is possible, based on a risk assessment, to deviate from obtaining the customer's identity information when providing assistance to customers with one-time activities that do not involve a transaction. A one-time activity could be, for example, an advisory task where there is no immediate prospect of the customer returning with new tasks, e.g., a one-time general advisory task in the investment area that does not take the customer's specific income and wealth situation into account. In such cases, there cannot be said to be an established fixed customer relationship or business relationship.

CCS must be able to demonstrate to the supervisory authority (the Danish Business Authority) that the specific case involved a one-time activity and that a risk assessment of the specific customer relationship led to the decision not to conduct KYC-procedures.

4.4 Verification of Costumer Information

Verification of identity information must be obtained in connection with the conclusion of agreements with new investors in AIFs and must be done through a source other than the customer. The verification of the beneficial owners' identity information can, if necessary, be carried out during the establishment of the business relationship, so as not to disrupt normal business operations, and where there is limited risk of money laundering or terrorist financing. In such cases, the verification must be carried out as soon as possible after the first contact.

If it is not possible to obtain the required information when conducting KYC-procedures, no further transactions may be conducted with the customer, and it must be investigated whether a report should be made to the Danish Financial Intelligence Unit (hereinafter "DFIU"). For reports to DFIU, see section 7.2.

If CCS becomes aware that the obtained information is insufficient and cannot be updated, CCS must take appropriate measures to mitigate the risk of money laundering and terrorist financing and positively determine whether the business relationship should be terminated as a result.

4.5 Power of Attorney

If a person states that they are acting on behalf of a customer, or if there is doubt as to whether a person is acting on their own behalf, CCS must identify the person, and their identity must be verified through a reliable and independent source. CCS must ensure that physical or legal persons acting on behalf of a customer are authorized to do so, unless the person is a lawyer licensed in this country or another EU or EEA country.

5 Enhanced or Simplified Requirements

If CCS assesses that there is an increased risk of money laundering or terrorist financing in a given situation, CCS must conduct enhanced KYC-procedures. This may be the case if the customer or the customer's beneficial owner originates from a country listed on the European Commission's list of countries with increased risk of money laundering[5] or if the customer, either directly or through the beneficial owner, is a politically exposed person (PEP) or closely associated with such a person. Examples of high-risk factors are listed in Appendix 1a to this policy.

If the customer is directly or indirectly a politically exposed person, CCS must ensure that the origin of the funds and assets involved in the transaction can be identified.

Enhanced KYC-pocedures mean that CCS must take additional measures to manage the increased risks associated with the customer relationship. There cannot be an exhaustive list of enhanced KYC-procedures, but as a general rule, increased monitoring of the customer must always be implemented to determine whether anything suspicious is occurring. This can also be done by requesting additional information or conducting KYC-procedures more frequently.

[5] https://www.finanstilsynet.dk/finansielle-temaer/hvidvask/risikovurdering-af-lande

CCS can also conduct simplified KYC-procedures if the risk of money laundering is limited. Low-risk factors are listed in Appendix 1a to this policy. The simplified risk assessment must be carried out before the simplified KYC-procedure is implemented. Simplified KYC-procedures may involve verifying the customer's identity information based on a single independent and reliable source, or CCS may assess the purpose of a business relationship itself.

CCS conducts a risk assessment of its customers when a business relationship is established or when an existing customer requests assistance with a new task and where the existing risk assessment on the customer is not updated. The risk assessment is performed via the digital tool Penneo KYC and includes questions as listed in Appendix 2. If a risk assessment results in a medium or high risk (i.e., not low), a decision must be made on whether increased monitoring is required to mitigate the money laundering risk.

5.1 Political Exposed Persons (PEPs)

CCS determines whether a customer or the customer's beneficial owner is a politically exposed person (hereinafter PEP). Furthermore, CCS must take reasonable measures to identify whether customers in CCS are closely associated to PEPs.

A PEP is a person who holds one or more of the high-ranking public positions listed in Appendix 1b. The definition is common to the entire EU but takes into account the different arrangements of the individual member states.

The Danish Financial Supervisory Authority's list contains information on the name, affiliation, and date of birth of domestic PEPs and aims to ensure consistency in the use of the definition for the covered individuals mentioned above.

The list indicates current PEPs. CCS must therefore continuously monitor whether customers have become PEPs.

Close associates and close business partners of a PEP should not be regarded as PEPs solely because of their connection to a PEP. Close associates and close business partners who are customers of CCS must be identified because they may benefit from or be misused in connection with money laundering, etc.

Close associates of a PEP: A politically exposed person's spouse, registered partner, cohabitant, or parent, as well as children and their spouses, registered partners, or cohabitants.

Close business partner of a PEP:

- A natural person who is the beneficial owner of a company or other legal entity together with one or more politically exposed persons.
- A natural person who otherwise has a close business connection with one or more politically exposed persons.
- A natural person who is the sole beneficial owner of a company or other legal entity that is known to have been established for the benefit of a politically exposed person.

CCS must take reasonable measures to identify customers who are close associates or close business partners of PEPs. This can be done by asking the PEP, if the PEP is also a customer of the company,

whether they are aware that close associates or close business partners are also customers. It can also be done by CCS, e.g., by fulfilling the general requirements for customer knowledge by searching the internet or using a commercial service provider that offers such information, etc.

CCS must carry out enhanced monitoring until CCS no longer assesses that the person poses an increased risk of money laundering and corruption. If the customer is no longer considered a PEP due to their position, CCS must, for at least 12 months after the person's PEP status ends, assess whether there is an increased risk associated with the person. This does not apply to close associates and close business partners of PEPs.

6 Information from Third Parties

The information that must be obtained in connection with the establishment of a business relationship, cf. section 4.2 above, can be omitted if it is provided by companies or persons covered by the AML Act (exhaustively listed in section 1, subsection 1, of the Act).

This would be the case, for example, if the information is provided by (i) financial institutions (banks, insurance companies, etc.), (ii) auditors, (iii) lawyers, and (iv) other real estate agents. The same applies if the information is provided by a company or person in an EU or EEA country that is subject to requirements equivalent to the rules of the AML Act.

Although the information has been obtained by such companies or persons, CCS can always request a copy of the identity and verification information or other relevant documentation about the customer or the beneficial owner.

CCS always retains responsibility for compliance with the AML Act, even if the information is provided by a third party.

7 Key Anti-Money Laundering Obligations

7.1 Investigation and Recording Obligation

If CCS encounters complex and unusually large transactions, CCS must investigate the background and purpose of such actions. The same applies to all unusual transaction patterns and activities that do not have a clear economic or demonstrably legal purpose, to determine whether there is suspicion or reasonable cause to believe that these have or have had connections to money laundering or terrorist financing. If deemed relevant, CCS should expand monitoring or activities to determine whether the transactions or activities appear suspicious. The results of CCS's investigations must be recorded and stored.

The basis of an investigation of suspicion will be to compare the information CCS has about the customer (information about the purpose of the business relationship and its extent) with what appears suspicious. In this connection, it may be necessary to contact the customer to obtain information about the purpose of the transaction or activity. If the customer's explanation is insufficient to dismiss the suspicion, it may be necessary to ask the customer for documentation to support the explanation. If CCS assesses that an inquiry would inform the customer that CCS has suspicions and is therefore conducting an investigation, or if CCS otherwise does not wish to contact the customer about the matter, CCS must report to the DFIU

(see below under section 7.2) if the suspicion cannot be dismissed. It is not sufficient for the suspicion to be merely weakened; it must be fully dismissed.

7.2 Reporting Obligation

If CCS becomes aware of, suspects, or has reasonable reason to believe that a transaction, funds, or an activity has or has had connections to money laundering or terrorist financing, CCS must immediately report to the Danish Financial Intelligence Unit (DFIU). CCS must first register as a user on the site to be able to make a report. A suspicion and submission of a report to the DFIU must be based on assessments of the specific situation, considering the nature of the actions and their difference from normal customer actions, omissions, and other distinctive and atypical conditions of the customer, which collectively draw attention to a possible attempt to conceal the origin of funds that are believed to be of a criminal nature. If suspicion arises as to whether a customer has a connection to terrorism, CCS will check whether the customer appears on EU official terror lists and the EU Sanctions Map. If this is the case, CCS will report to the DFIU.

CCS must refrain from assisting a transaction until reporting to the DFIU has been made if there is suspicion of money laundering or terrorist financing or reasonable cause to believe that the transaction is connected to money laundering or terrorist financing.

If an employee finds grounds to report to the DFIU because there is money laundering or a connection to terrorism, the employee must discuss the report with the person responsible for anti-money laundering obligations in the business. The person responsible for the business will then be the one to report to the DFIU. If a report is made, the business must keep confidential that a report has been made.

7.3 Record-Keeping Obligation

CCS must retain the following collected information:

- Information obtained in connection with compliance with KYC-procedures, including identity and verification information and copies of the presented identification documents.
- Documentation and records of transactions conducted as part of a business relationship or a one-time transaction.
- Documents and records relating to investigations conducted under section 7.1.

The information must be retained for at least five years after the termination of the business relationship or the specific transaction. The same applies to personal data.

8 Fund Transfers

Payments from customers to CCS must be made as a bank transfer or other electronic transfer (e.g., giro transfer). CCS does not accept cash payments unless they are insignificant amounts. When CCS receives payments, CCS must verify that the payments and payment information can be attributed to a customer relationship or a transaction. If the information does not match, e.g., if CCS is to receive payment from

an unknown party, CCS must resolve the discrepancy and dismiss any suspicion of money laundering in connection with it.

9 Confidentiality and Liability

Reports to the DFIU made in good faith or to prevent suspicious transactions do not impose any form of liability on CCS. Disclosure of information in such situations is not considered a breach of confidentiality. Violation of the rules in the AML Act may be punishable by a fine. In the case of particularly serious or extensive intentional violations, the penalty can increase to imprisonment for up to 6 months. Participation in money laundering can be punished by imprisonment for up to 8 years under sections 290 or 290a of the Penal Code, while participation in terrorist financing can be punishable by life imprisonment under section 114 of the Penal Code.

In addition to the consequences resulting from the general rules of the law, a violation of the relevant set of rules, depending on the nature of the violation, may be considered a material breach of the employment relationship between an employee and CCS.

10 Ongoing Training

CCS is responsible for ensuring that employees are made aware of the obligations arising from the AML Act and this policy. The obligation applies to all employees involved in operations and/or holding functions where there is a potential risk of money laundering and terrorist financing. CCS must continuously and at least once a year ensure that relevant employees and management receive adequate training in the requirements of the AML Act.

11 Employee Screening

CCS must prevent employees from misusing their position for money laundering and terrorist financing or assisting in this, which is achieved, among other things, by screening employees. Screening is carried out by the HR responsible in the business. Employee screening consists of the following two parts:

- Ensuring that the employee has not been convicted of a criminal offense that increases the risks of the person misusing their position.
- Ensuring that the employee has sufficient qualifications in the anti-money laundering area to hold the position.

Employees in leadership and/or trusted positions will also be particularly relevant for screening. The content and specific procedures for employee screening are detailed in Appendix 3.

12 Control

To comply with and monitor the fulfillment of the requirements of the AML Act, a controls have been prepared. When establishing and changing a customer relationship, controls in Penneo KYC are made based on the questions in Appendix 2 unless it is otherwise ensured that the mentioned anti-money

laundering obligations are observed. The control questions must be registered/stored together with the other obtained information. Furthermore, CCS must continuously conduct random checks to ensure that this policy is adhered to in daily operations. Checks must be carried out in a way that can be documented.

The policy should generally be updated once a year. If the business model changes due to new activities or if new types of risks of misuse of CCS arise, the policy must also be updated even if a year has not passed since the last update of the policy.

13 Regulatory Oversight

The Financial Supervisory Authority oversees CCS's compliance with the AML Act. CCS must therefore always provide the Financial Supervisory Authority with the necessary information. The Financial Supervisory Authority is entitled, if the purpose requires it, to access CCS at any time with proper identification and without a court order to obtain information. This may also occur through inspection visits from the Financial Supervisory Authority. If the Financial Supervisory Authority's oversight of CCS's compliance with the anti-money laundering rules triggers a reaction from the authority, such a reaction may be published on the Financial Supervisory Authority's website, and depending on the nature of the violation, it may be transferred to police investigation.

14 Reporting to the Board of Directors

CCS reports to the Board of Directors once a year on matters covered by this policy. The Board of Directors must be informed as soon as possible of any significant breach of the policy or any underlying business processes.

15 Review

The policy must be reviewed and, if necessary, adjusted by CCS's Board of Directors at least once a year to ensure that it continuously covers all relevant areas associated with CCS's business model. Any change to the policy must be updated on CCS's website.

****

Approved by the Board of Directors 2nd of September, 2024

APPENDICES

Appendix 1a. Risk Factors

The following factors and types of documentation characterize situations that potentially involve a limited risk:

1. **Customer Risk Factors:**
    - Publicly traded companies subject to disclosure requirements (either under stock exchange rules or legislation or enforcement measures) that require companies to ensure appropriate transparency regarding beneficial ownership.
    - Public administrations or enterprises.
    - Customers residing in geographical areas with lower risk as described below in geographical risk factors.
2. **Risk Factors Related to Products, Services, Transactions, or Delivery Channels:**
    - Life insurance policies where the annual premium is low.
    - Pension insurance policies with no early surrender option and where the policy cannot be used as collateral.
    - Pension schemes or similar that pay pensions to employees and where contributions are made through payroll deductions and the rules of the scheme do not allow the transfer of a member's rights under the scheme.
    - Financial products or services that provide well-defined and limited services to certain customer types with the aim of promoting financial inclusion.
    - Products where the risk of money laundering and terrorist financing is controlled by other factors such as spending caps or transparency regarding ownership (e.g., certain types of electronic money).
3. **Geographical Risk Factors:**
    - EU or EEA countries.
    - Third countries with effective anti-money laundering and terrorist financing measures.
    - Third countries identified by reliable sources as having a limited level of corruption or other criminal activity.
    - Third countries that, based on credible sources such as mutual evaluations, detailed assessment reports, or published follow-up reports, have anti-money laundering and terrorist financing requirements consistent with the FATF 2012 recommendations and that effectively implement these requirements.

The following factors and types of documentation characterize situations that potentially involve an increased risk:

- **Customer Risk Factors:**
    - Business relationships that exist under unusual circumstances.
    - Legal persons or legal arrangements that are personal wealth management companies.
    - Companies with nominee shareholders or bearer shares.
    - Cash-based businesses.
    - A company's ownership structure that appears unusual or too complex given the company's business activities.
    - Customers residing in geographical areas with higher risk as described below in geographical risk factors.
- **Risk Factors Related to Products, Services, Transactions, or Delivery Channels:**
    - Private banking.
    - Products or transactions that can promote anonymity.
    - Business relationships or transactions without direct contact and without security measures such as electronic signatures.
    - Payments from unknown or unrelated third parties.
    - New products and new business procedures, including new delivery mechanisms and the use of new technologies or technologies under development for both new and existing products.
- **Geographical Risk Factors:**
    - Countries identified by reliable sources, such as mutual evaluations, detailed assessment reports, or published follow-up reports, as countries that do not have effective anti-money laundering and terrorist financing arrangements.
    - Countries identified by reliable sources as countries with a significant level of corruption or other criminal activity.
    - Countries subject to sanctions, embargoes, or similar measures taken by, for example, the EU or the UN.
    - Countries that finance or support terrorist activity or that host known terrorist organizations.

Appendix 1b. PEPs

The definition of Danish PEPs is as follows:

- Head of state, head of government, minister, and deputy minister or assistant minister. In Denmark, this includes ministers as well as department heads.
- Members of parliament or members of equivalent legislative bodies. In Denmark, this includes members of the Folketing and Danish members of the European Parliament.
- Members of the governing bodies of political parties. In Denmark, this includes the central boards or equivalent high-level bodies under the statutes of political parties represented in the Folketing.
- Supreme court judges, members of constitutional courts, and other high-level judicial bodies whose decisions are subject to further review only under extraordinary circumstances. In Denmark, this includes supreme court judges and Danish judges at international courts.
- Members of audit courts and the highest management bodies of central banks. In Denmark, this includes the directorate of the National Bank of Denmark, Danish state auditors, and the Danish member of the European Court of Auditors.
- Ambassadors, chargé d'affaires, and high-ranking officers in the armed forces. In Denmark, this includes the top commanders in the armed forces, specifically defined as the chief of defense, deputy chief of defense, service chiefs, and ambassadors to Danish embassies.
- Members of the administrative, managerial, or supervisory bodies of state-owned enterprises. In Denmark, this includes the board of directors and the CEO of companies where the state owns 50% or more or otherwise has actual control over the company. Subsidiaries of such state-owned companies are not covered by the concept. Self-governing institutions that are wholly or partly financed through the Finance Act are also not covered by the concept.

  The definition also includes the director of agencies and members of the board of agencies where this group of people has actual decision-making authority.
- Directors, deputy directors, board members, and persons with equivalent positions in international organizations. In Denmark, this includes individuals nominated, appointed, or employed by the government, a ministry, or a minister in an international organization established by the conclusion of a formal international political agreement.

Appendix 2. Questions for Control and Risk Assessment of Customers in Penneo KYC

Questions to customers:

1. Are you a politically exposed person (PEP)?

2. Is Denmark the only country where you hold citizenship?

3. Is Denmark the only country where your investment company is taxable?

4. In which countries is your investment company taxable?

5. What is the purpose of the investment with Cresco Capital Services A/S?

6. Where do the funds invested in the alternative investment fund(s) come from?

7. Do you or your investment company have customers? If yes:
    - What type of customers? (Private individuals, private companies, public entities, associations).
    - Where are the customers located? (Denmark, Scandinavia, EU/EEA, countries outside the EU/EEA).
    - How do you/the company interact with its customers? (In person, online, by phone).
    - Do customers ever pay in cash? If yes, how often?
    - Do you/the company have customers who pay more than DKK 10,000 per order?
    - Is cash payment from customers common in your/the company's industry?

8. Do you/the company receive products or services from suppliers (e.g., accountants, lawyers, or similar)?

9. Are your/the company's suppliers located in any of the following countries?
    - Syria, Iran, Congo, Venezuela, Libya, Russia, Ukraine, or North Korea?

10. Do you/the company ever pay suppliers in cash?

11. Do you/the company ever pay suppliers more than DKK 10,000 per order?

12. Do you/the company use any providers other than the bank for money transactions? Which ones?

Internal questions for risk assessment:

1. Is the ownership or control structure unusual or complex in a way that increases the risk of money laundering and/or terrorist financing?

2. Is the customer's industry, goods, or services associated with an increased risk of money laundering and/or terrorist financing?

3. Does the customer operate in geographic markets that pose an increased risk of money laundering and/or terrorist financing?

4. Does the customer conduct money transactions with countries outside the EU/EEA that increase the risk of money laundering and/or terrorist financing?

5. Is the customer's cash holdings and/or transactions larger than normal for the industry?

6. Is the customer asking for unusually creative solutions to avoid or reduce the payment of mandatory taxes and VAT? If yes, do you assess that this increases the risk of money laundering and/or terrorist financing?

7. Does the customer's use of our services – including the composition and any opt-outs – give rise to an increased risk of money laundering and/or terrorist financing?

8. Describe the company's activities as well as the purpose, intended nature, and scope of the customer relationship.

9. With your knowledge of the purpose and intended nature of the customer relationship, is there an increased risk of money laundering and/or terrorist financing?

10. Do we know that any of the beneficial owners have other businesses or relationships that give rise to an increased risk of money laundering and/or terrorist financing, including tax evasion?

11. How high is the risk of money laundering or financing of terrorism that you assess to be associated with this cooperation? (High, medium, low)

Appendix 3. Employee Screening

According to the Financial Supervisory Authority's guidance on the anti-money laundering area, screening of employees must take place before employment for those employees where there is a risk of misuse of the position for money laundering or terrorist financing, including assistance with this. The screening, therefore, applies to CCS employees who are involved with customers and the purchase of properties.

CCS can, for example, verify this by requesting the employee to submit their private criminal record. Not all criminal offenses increase the risks of the person misusing their position. For example, convictions for financial crime and gross tax evasion would generally increase the risk, whereas, for example, driving under the influence may not necessarily disqualify an employee from holding the position in question. Thus, an assessment must be made regarding the types of offenses that increase the risk. However, it is essential that the screening is always based on a risk-based approach and is proportional to the employment relationship and the specific function that the employee will or is performing.

CCS must determine which functions are relevant to be subject to screening procedures. It is not required that all employees be screened, but there must be an assessment of which function the employee will hold. For example, it would not be relevant for employees who do not perform functions that ensure compliance with the AML Act. However, screening of employees will always be relevant if the employee performs a function where they can directly or indirectly misuse their position to assist in money laundering or terrorist financing. Employees in leadership and/or trusted positions will also be particularly relevant for screening.

CCS must also ensure, on a risk-based basis, that it becomes aware if an employee is convicted of a criminal offense during employment that increases the risks of the person misusing their position. This can be done, for example, by:

- CCS inserting a disclosure obligation in its employment contracts, so the employee must inform if they are convicted of a criminal offense during employment.
- CCS, at a certain interval (e.g., annually) or by random checks, requests the employee to present their private criminal record and stores documentation that the criminal record has been presented.

The proposed procedures are examples from the Financial Supervisory Authority's practice, and they do not necessarily reflect a practice that CCS is required to follow, but CCS can assess the most appropriate procedure for CCS depending on the specific situation to achieve the purpose of the rules on screening. If CCS chooses to screen at a certain interval, CCS can set the interval based on a risk assessment, i.e., an assessment of the risk.