Anti-Money Laundering and Counter-Terrorist Financing Policy

Table of contents

1. Introduction. The Concept of Money Laundering and Terrorist Financing. Purpose of the Policy

C&F S.A. and its subsidiaries and affiliated companies do not engage in practices aimed at money laundering, terrorist financing, or other financial crimes, and firmly condemn such activities. We expect the same conduct from our employees, associates, consultants, business partners, and all individuals, bodies, and organizations we interact with in the course of our professional and business activities.

The term “money laundering” covers all activities related to the movement of funds used in illegal operations. This applies both to financial resources derived from illegal activities and to legal funds intended to finance unlawful operations (also referred to as reverse money laundering).

Primarily, this includes actions aimed at introducing money or other assets derived from illegal sources into legitimate circulation, or using such funds to finance illegal activity. In most cases, it concerns proceeds from organized crime, including drug trafficking, extortion, racketeering, fraud, and scams; organized hacking and other forms of cybercrime; illegal arms trade; other types of unlawful trade (including sanctions evasion); human trafficking; war crimes; forced labor; smuggling; illegal gambling; counterfeiting of money; tax fraud; counterfeiting of goods; and other forms of organized criminal activities. It also includes all types of financial and economic crimes as well as acts of corruption. Furthermore, it pertains to concealing financial flows intended to finance terrorism, i.e., funding activities designed to unlawfully coerce a government or international organization into taking or refraining from certain actions, or to seriously destabilize or destroy the political, constitutional, economic, or social foundations of a state or international organization—even when such funding originates from legal sources.

Money laundering and terrorist financing are prohibited by law, morally unacceptable, and harmful to social and economic relations. With due regard for applicable Polish, European, and international law; the welfare of C&F S.A. and its affiliated companies; standards of good business conduct; the expectations of our business partners; and above all, our own values and ethical principles, we have implemented this policy (hereinafter referred to as the “**Policy**”) to ensure that our operations do not support or participate in any practices related to money laundering, terrorist financing, or other financial crimes.

The specific implementation of this Policy is governed by detailed procedures in force at C&F S.A. and its affiliated companies (if such procedures have been adopted).

C&F expects all obligated persons and counterparties (as defined below) to comply with this Policy to the extent possible and necessary, taking into account the nature, type, and scale of their activities, and to implement appropriate procedures.

2. Defined Terms

For the purposes of this Policy, the following terms shall have the meanings defined below:

- **money laundering** – activities related to money laundering as well as terrorist financing, as described in the Introduction of this Policy;
- **C&F** – C&F S.A. and its subsidiaries and affiliated companies;
- **obligated person** – C&F S.A. and/or its subsidiaries and affiliated companies, as well as members of C&F's governing bodies, employees, associates, consultants, and subcontractors;
- **counterparty** – a business partner of C&F, including a supplier, subcontractor, or client, as well as any other persons or organizations with whom C&F interacts in the course of its business operations;
- **irregularity** – the occurrence of money laundering, or any violation and/or potential violation by an obligated person or counterparty of applicable laws or internal regulations related to money laundering, including this Policy, or a situation that facilitates the occurrence of such violations. An irregularity also includes a red flag;
- **red flag** – any information or circumstance indicating a high probability that money laundering activities have taken place, or that an obligated person or counterparty may be engaged in conduct that shows signs of irregularity concerning anti-money laundering procedures.

3. Prohibition of improper practices and obligation to take precautionary measures

Obligated persons are strictly prohibited from engaging in any activities related to money laundering within the scope of C&F's operations or in any connection with C&F's business.

In the event that another entity is found to be engaged in money laundering activities, or if there is a strong suspicion that such activities have occurred—and the doubts cannot be resolved—C&F shall:

- refrain from entering into any business relationship with such entity;
- refrain from carrying out any transaction with such entity;
- immediately terminate any existing business relationship, including any contracts in force;
- assess the legal necessity or advisability of reporting the suspected money laundering activity to the competent public authority, and based on the outcome of that legal assessment, submit such a report if appropriate.

4. Due diligence measures

As part of its due diligence measures, C&F undertakes actions to identify certain counterparties and verify their identity by applying the following procedures:

- ***Know Your Customer*** (KYC) Procedure – applies to counterparties and all entities for whom C&F performs work or services as part of its business operations;
- ***Know Your Vendor*** (KYV) Procedure – applies to counterparties and all entities that perform work or services for C&F as part of their business operations.

These procedures include the stages of entity and transaction identification as well as risk assessment, and are carried out:

- prior to initiating cooperation with the counterparty,
- in the event of changes to key parameters of the cooperation with the counterparty, including any changes to the counterparty’s identification data during the course of the relationship.

1. **Entity Identification**

   a) For natural persons:

   - Collection of the counterparty's business activity data;
   - Verification of the counterparty's identity.

   b) For legal entities and other collective entities:

   - Collection of the entity's registration data;
   - Collection of information on the method of representation and the persons authorized to represent the entity;
   - Collection of information on the counterparty's ownership and control structure (optional);
   - Identification of the entity's ultimate beneficial owner (optional).

2. **Possible scope of verification**

   - Verification of the tax identification number;
   - Verification of whether the counterparty operates in a high-risk jurisdiction;
   - Identification of the counterparty's actual business activity and method of operation;
   - Identification of the payment beneficiary;
   - Verification of whether the counterparty is, or is closely associated with, individuals from countries with a high prevalence of corruption;
   - Verification of whether the counterparty or members of its governing bodies are, or are closely associated with, individuals who hold or have held prominent public functions in any country or on the international stage. This verification will be conducted in situations required by C&F's clients or partners.

3. **Collection of the Counterparty's Transaction Requirements**

   C&F collects information about the planned transaction, in particular regarding the counterparty's requirements concerning:

   a) the subject and purpose of the transaction;

   b) the remuneration and method of payment;

   c) the place of performance.

4. **Risk Assessment**

   Risk assessment includes conducting the following analysis based on the collected data and any publicly available information:

   a) evaluation of the likelihood that the counterparty may commit offenses related to money laundering and terrorist financing: (1) verification against sanctions lists; (2) where required by law – verification of certificates from the national criminal record;

   b) estimation of the risk posed by establishing cooperation with the given counterparty in terms of potential damage to C&F's reputation or other harm;

   c) assessment of the completeness of the information held regarding the purpose and intended nature of the business relationship with the counterparty (transaction analysis);

   d) evaluation of the ability to understand the counterparty's ownership and control structure;

   e) assessment of the impact of the counterparty's business location on the security of the transaction;

   f) estimation of the risk arising from conducting transactions with unusual parameters.

In cases where the actions described above give rise to doubts regarding the issues addressed in this Policy, or when the counterparty operates in sensitive industries particularly vulnerable to fraud, an enhanced risk analysis shall be conducted.

C&F may carry out the enhanced risk assessment with the involvement of external advisors or specialists providing services in this area.

5. Risk Management

Based on the conducted analysis and established risk assessment criteria, C&F may decide not to enter into or to terminate cooperation with the counterparty, or to apply additional measures to mitigate the risk.

5. Reporting of irregularities

Every obligated person should be attentive to the occurrence of red flags and other types of irregularities and is obliged to report any irregularities immediately. This particularly applies to the following situations and irregularities when:

- The counterparty or potential counterparty refuses to provide information enabling proper and complete identification in accordance with good Know Your Vendor / Know Your Customer practices, or provides information that does not correspond to the actual facts, or when there are reasonable doubts regarding the accuracy of their identification data;
- During the provision of services by C&F to a client, it becomes apparent that the client's activities involve money laundering, or it becomes clear that the client or persons acting in concert with or on behalf of the client are engaged in money laundering activities;
- During cooperation with the counterparty, a condition or situation is identified that may facilitate or lead to money laundering;
- Circumstances arise that directly indicate preparation for money laundering, including (a) a person's declaration of intent to engage in such conduct, or (b) any other instance of preparation, attempt, or commission of an offense related to money laundering.

C&F has established a procedure and methods for reporting irregularities and red flags.

Reports of irregularities or red flags can be made at C&F:

a) in person – to the person responsible for the financial area at C&F,

b) via the email address legal@candf.com.

Every properly made report, including anonymous ones, will be acknowledged. Addressing anonymously reported cases may be difficult or impossible if the information is incomplete and sufficient data cannot be obtained.

Reports made in good faith are treated confidentially and investigated with due diligence. The person making a report in good faith is entitled to protection, including identity protection. No person who reports in good faith can be held liable, regardless of the outcome of the investigation. Making a report in good faith must not negatively affect the reporter's situation through, for example, being passed over for promotion, demotion, denial of work assignments, reassignment to another workplace, salary reduction, or termination of employment or cooperation.

Reports made in bad faith will be assessed according to their legal and factual nature, and those making such reports will not be granted protection. Bad faith occurs when the reporter knows, or should know with due diligence, that the reported irregularities constitute false accusations or the report is based on false evidence.

6. Reviews and Continuous Improvement

1. Purpose, scope, and frequency of reviews

The AML Policy is reviewed annually or in the event of significant regulatory changes to ensure its compliance with applicable laws and best market practices. The reviews cover all aspects of the policy, including customer identification procedures, transaction monitoring, and remedial measures applied to suspicious activities.

2. Effectiveness analysis and reporting

At the request of C&F's management, the effectiveness of AML procedures is evaluated, and the review results are documented and subsequently reported to management or the relevant supervisory personnel.

3. Roles and responsibilities

Policy reviews are conducted by a person or persons appointed by C&F's management who possess appropriate knowledge and competencies in finance, law, and security to enable effective analysis and implementation of changes.

4. Commitment to Continuous Improvement

C&F is committed to enhancing its AML capabilities through, among other things, training staff who interact with counterparties, striving to implement technologies supporting the detection of suspicious transactions, and adopting industry best practices to increase the effectiveness of AML procedures.