Prevention of Money Laundering and Terrorist Financing Policy

December 2024

Version 4.0

	Department in charge	Date
Made by:	CTT Compliance Function Payshop Compliance Function	06/12/2024
Verified by:	AML Officer of CTT AML Officer of Payshop Payshop Risk Function	06/12/2024
Appraised by:	Audit Committee (CAUD)	11/12/2024
Approved by:	Board of Directors (BoD)	12/12/2024

Version control

Version	Date	Editor	Approving body	Date of entry into force	Remarks
1.0	19/12/2018		BoD	02/01/2019	First version
2.0	23/12/2021		BoD	10/02/2022	Changes resulting from the periodic review
3.0	20/12/2022		BoD	20/12/2022	Changes resulting from the periodic review
4.0	06/12/2024	Compliance Function	BoD	12/12/2024	Changes resulting from the periodic review

TABLE OF CONTENTS

1. Acronyms

Acronym	Meaning
AML	Anti-Money Laundering
AML Officer	Anti-Money Laundering Officer
AML/CFT	Prevention of Money Laundering and Terrorist Financing (Anti-Money Laundering/ Combating the Financing of Terrorism)
ARI/Golden Visa	Residence Permit for Investment
BdP	Bank of Portugal
CDD	Customer Due Diligence
DCIAP	Central Department for Investigation and Penal Action of the Public Prosecutor's Office
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit of the Criminal Investigation Police
IFM	Immediate Family Members
KYC	Know Your Customer
KYCC	Know Your Customer 's Customer
KYP	Know Your Process
KYT	Know Your Transaction
ML/TF	Money Laundering and Terrorist Financing
PEP	Politically Exposed Person
PGR	Public Prosecutor's Office
PREA	Persons Known to be Close Associates
RBA	Risk-based approach
RCBE	Central Register of Beneficial Owners
RPB	Report on the Prevention of Money Laundering and Terrorist Financing
TCPP	Political or Public Office Holders

2. Introduction

The purpose of this Policy for the Prevention of Money Laundering and Terrorist Financing (ML/TF), hereinafter referred to as the "Policy", is to (i) set out how the prevention of money laundering and financing of terrorism should be carried out in CTT - Correios de Portugal, S.A. and Banco CTT Group, which includes Banco CTT, S.A. and Payshop (Portugal), S.A., hereinafter "CTT Group"[1], (ii) explain the general duties to be observed by the member entities that are subject to the provisions of Law 83/2017 of 18 August, as amended[2], and other applicable legislation and regulations within the scope of the measures to combat money laundering and terrorist financing, (hereinafter referred to as "Obliged Entities of the CTT Group"), as well as (iii) describe the governance model, indicating their functions and responsibilities in relation to the Prevention of Money Laundering and Terrorist Financing.

This Policy also aims to formalize the practices related to the prevention of the use of the financial system by persons or entities subject to sanctions in accordance with the provisions of Law 97/2017 of 23 August, as amended, and Law 58/2020 of 31 August, which regulates the application and enforcement of restrictive measures approved by the United Nations (UN) and the European Union (EU) and establishes the system of sanctions applicable to the violation of these measures.

With this Policy, we underline the special duty of all employees of the Obliged Entities of the CTT Group, within the scope of their duties and daily activity, to take into account and act in accordance with the legislation and regulations in force on BCFT, as well as with the guidelines, rules and internal regulations on the matter.

3. Objectives and scope

The Obliged Entities of the CTT Group assume as an inseparable condition of their business model the adoption of internal procedures aligned with the best practices and high international standards to fight ML/TF, requiring all members of their corporate bodies and all their Employees to comply, without any reservations or limitations, with those procedures, fostering a culture of integrity, risk assessment associated with each Product, Customer, Counterparty or operation and the immediate reporting of any signs of suspicious practices or behaviour in terms of ML/TF.

[1] The Institutional Information on the Entities indicated can be found in item 13 of this Policy.

[2] Law 83/2017 of 18 August updated by Law 58/2020 of 31 August and Law 99-A/2021 of 31 December.

Such report shall be addressed to the head of the Compliance Function, or the Anti-Money Laundering Officer (AML Officer) provided for in Article 16 of the aforementioned Law 83/2017.

In the Obliged Entities of the CTT Group, the prevention of ML/TF comprises the following aspects:

- Ensure that the entire organisation recognises the importance of assessing risk and preventing its involvement in ML/TF practices;
- Ensure that each and every Employee with responsibilities for accepting and retaining Clients, Counterparties or managing transactions knows and acts in accordance with the ML/TF prevention procedures adopted;
- Continuously monitor compliance with all legal and regulatory requirements on prevention of ML/TF and sanctions compliance, which include the restrictive measures approved by the UN and EU;
- Guarantee firm, rigorous and timely action on any suspicion of ML/TF and compliance with sanctions, thus preserving the reputation of the Group and the CTT brand and contributing to maintaining the trust of Customers, Counterparties, Regulatory Authorities and other stakeholders;
- Immediately report situations of well-founded suspicion of ML/TF, or those related to restrictive measures, to the competent authorities, ensuring full cooperation with them.

This Policy is applicable to any and all processes that are part of the CTT Group's activity, the execution of which is directly or indirectly subject to the legal and regulatory requirements in force on the prevention of ML/TF, covering, in particular, the processes related to (i) Customer and Counterparty Management; (ii) insurance mediation; (iii) the postal activity (the issuing and payment of postal money orders); (iv) Document Management; and, in the case of Payshop, (v) payment services and financial products.

For further details on the responsibilities and obligations related to the Compliance function, please refer to the function's regulations on the prevention of money laundering and terrorist financing.

4. Responsibilities

The Board of Directors or equivalent body is the owner and responsible for the prevention of ML/TF, and shall define, implement, supervise and periodically review the strategic model for the management of ML/TF risk and compliance with sanctions. It shall ensure its optimization and

adequacy, through the existence of methodologies, means, processes and procedures appropriate to the characterization, implementation and supervision of the ML/TF practices adopted by the Obliged Entities of the CTT Group.

It is incumbent upon the Management Body of each Obliged Entity of the CTT Group, as the body responsible for the Policy:

- To approve the Policy, as well as any amendments thereto;
- To ensure the alignment of the Policy with the mission, vision and strategic objectives of the CTT Group, as well as with the regulations and recommendations of the regulatory entities in matters of ML/TF and compliance with sanctions;
- To ensure the application of the Policy, as well as the effectiveness of the ML/TF prevention model implemented by the CTT Group;
- To ensure the adequacy of the Policy to the business and exposure to ML/TF risk and compliance with sanctions by the Obliged Entities of the CTT Group, considering the tolerated risk level previously defined;
- To confirm that all matters related to ML/TF prevention and sanctions compliance are identified, assigned and phased appropriately and in accordance with the governance model set out in the Policy.
- To approve the Report on the Prevention of Money Laundering and Terrorist Financing (RPB).
- To issue an overall opinion on the adequacy and effectiveness of the respective internal control system, within the specific scope of the prevention of money laundering and financing of terrorism.

It is incumbent upon the Executive Management Body of each Obliged Entity of the CTT Group:

- To become aware in advance the content of the Policy, as well as of any amendments thereto.

It is incumbent upon the Supervisory Body of each Obliged Entity of the CTT Group:

- To previously assess the Policy, as well as any amendments thereto;

- To debate the Report on the Prevention of Money Laundering and Terrorist Financing (RPB) with the Board of Directors;
- To issue an opinion on quality of the internal control system for the prevention of money laundering and terrorist financing.

It is incumbent upon the Compliance Department/AML Officer of each Obliged Entity:

- To promote, in conjunction with its counterparts of the other Obliged Entities, the review of the Policy at least every two (2) years, as well as interim amendments whenever:
    - it detects opportunities to improve the effectiveness and efficiency of the internal control system regarding the prevention of ML/TF and compliance with sanctions;
    - it finds that the Policy is outdated in view of new legal requirements or new recommendable practices regarding the combat of ML/TF and compliance with sanctions;
    - relevant changes occur in the products or services offered by the Obliged Entities of the CTT Group, in the target Customer segments or in the geographic areas where such entities operate and that have an impact on the Policy.

It is incumbent upon the Product Manager:

- To manage their product's ML/TF risk, as first-line risk taker, by enforcing the prevention of ML/TF policy through the implementation of ML/TF prevention processes, procedures and controls.

5. Addressees

This Policy is of general application to all the Obliged Entities of the CTT Group, without prejudice to the cases in which, by legal or statutory imposition, certain companies must have their own more demanding policies, approved by the respective management bodies.

In companies that are merely subsidiaries, over which the CTT Group has no powers of control, the CTT Group will seek to promote the adoption of this policy or of principles and commitments equivalent to those contained herein, so that companies that have their own policies define them in terms that are no less demanding than those defined directly by the CTT Group.

This Policy is addressed to all members of the corporate bodies and Employees, and binds them automatically, for as long as they exercise functions, or provide services, in or for the Obliged Entities of the CTT Group.

6. Revision and updating

This Policy shall be reviewed at least on every two (2) years, in order to ensure that it remains current and appropriate to the fulfilment of its purpose and that it is adequate to the internal and external environment of the Obliged Entities of the CTT Group.

Whenever deemed necessary, the document may be updated on an interim basis, namely due to the entry into force of new legal requirements.

7. Communication

The Policy is fully communicated and made available at all times to its Addressees (see Chapter 5. Addressees), on the intranet of each entity. In addition, it is published on the respective website, in accordance with the procedures set out in the internal Manual.

In addition, the heads of each functional area, as the first lines of defence, are responsible for ensuring that this policy is reflected in the respective processes and procedures, where applicable.

8. Strategic model

The obligated entities of the CTT Group are committed to maintaining adequate policies, procedures and internal controls to comply with the laws and regulations on the prevention of ML/TF.

The policies and procedures of the CTT Group Obliged Entities are developed on the basis of regulations and respective controls and are designed to address the Company's risk in all sectors in which the Group conducts business. These policies are reviewed periodically, and updates are made accordingly.

8.1. General Principles

The Obliged Entities of the CTT Group assume the following as general principles of their ML/TF risk management strategy and compliance with sanctions:

1. The implementation of the necessary procedures to ensure the prevention, management and mitigation of ML/TF risk and compliance with sanctions in accordance with the risk appetite and tolerance level approved by the Obliged Entity, associated with the establishment and maintenance of Business Relationships and execution of Occasional Transactions.
2. Compliance with the legal requirements, regulations and national and international recommendations in force and applicable to the operating reality of the Obliged Entities with regard to the duty of identification and diligence in the establishment of Business Relationships and Occasional Transactions.
3. The disclosure and availability to the addressees, regardless of the medium adopted, of the contents of the Policy and of the procedures related to the prevention of ML/TF and Compliance with sanctions, at each moment in force.
4. The promotion of training on the prevention of ML/TF and compliance with appropriate sanctions to all addressees of the Policy.
5. The proactive monitoring of compliance with the Policy and related procedures.
6. The regular production of management reports to monitor the effectiveness of ML/TF prevention and sanctions compliance procedures.

8.2. Risk-based Management and Control Approach (RBA)

An effective risk management programme requires that risks are analysed and assessed and that reasonable controls are put in place if tolerance levels are exceeded.

The Obliged Entities of the CTT Group base their strategic model for the prevention of ML/TF on a risk-based approach, developing for that purpose a methodology that allows assessing the risk inherent to the type(s) of activity that they carry out, the typology and effectiveness of the implemented controls, culminating with the identification of the residual risk of ML/TF and compliance with sanctions, which must be in line with the entity's risk appetite.

The aim of the Risk Assessment is thus to establish priorities within the Group and clearly define areas of greatest risk, providing guidelines for mitigating them.

Such assessment is periodically reviewed and updated, and this practice leads not only to the identification of vulnerabilities but also a gauging of probability and impacts. This review/update will also reflect alignment with new guidelines that the various sector authorities may determine.

The result of the assessment of ML/TF risk and compliance with sanctions enables harmonised risk profiles to be created for Customers, Representatives, Beneficial Owners, products/services and/or operations and distribution channels, to identify them and to carry out differentiated due diligence according to the levels of risk in question.

Bearing in mind that risk profiles help determine whether a Customer, product, service, transaction or distribution channel entails a possible increased risk to the activity or reputation of the Obliged Entities of the CTT Group, the information collected on the Customers, their behaviour, transactional profile or the Occasional Transactions themselves will be considered, whenever possible, in the calculation and updating of risk degrees.

This approach includes the establishment of controls and mechanisms to monitor Customers, products/services, transactions and other relevant counterparties, which allow updating their degree of risk, when there are relevant situations regarding ML/TF and compliance with sanctions.

The ML/TF prevention governance model was built around a three-lines-of-defence approach, as shown in figure 1, where (i) the 1st line areas are those with direct contact with Customers, Consumers and underlying transactions, (ii) the 2nd line areas are for instance the Compliance Function/AML Officer function responsible for 1st line monitoring, and (iii) a 3rd line, if applicable, is the Internal Audit Function, responsible for examining and assessing the adequacy and effectiveness of the systems, procedures and standards that support the ML/TF prevention system. This is done particularly by carrying out effectiveness tests, ensuring that this evaluation is reported to the Structure Units responsible for them (in particular, the Compliance Function/AML Officer) and to the management bodies. The Internal Audit Function shall also issue recommendations based on the results of the assessments carried out on the methodologies, means, processes and procedures for preventing ML/TF, verifying their compliance and correct implementation.

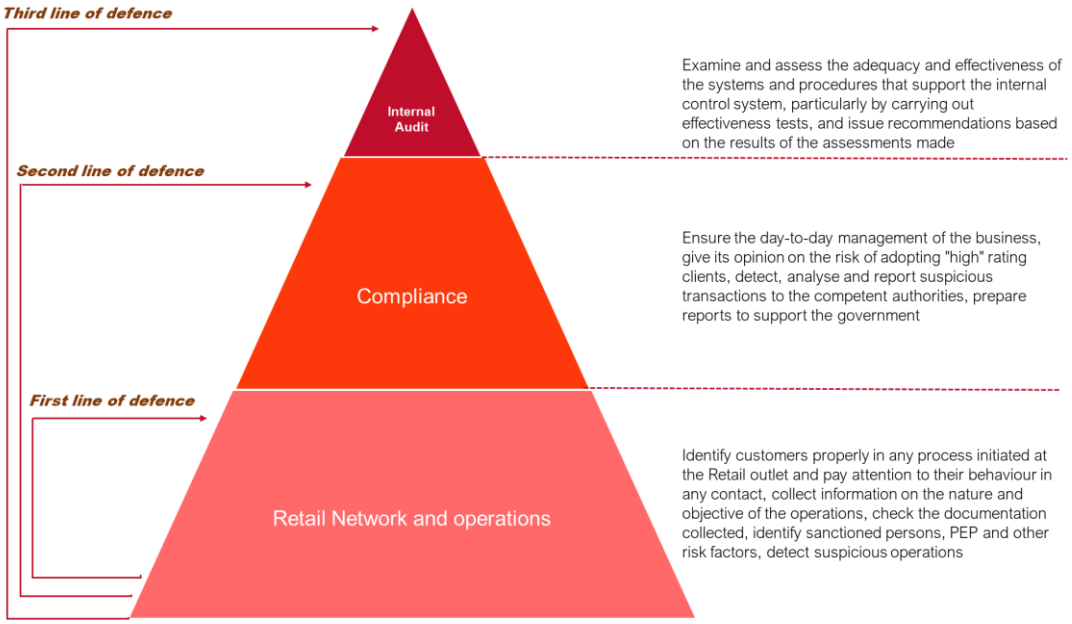

Figure 1 – Generic three-lines-of-defence approach

Each Obliged Entity shall define and implement an internal control system adapted and proportional to its size, complexity and operational reality. This system allows monitoring and ensuring compliance with legal and regulatory standards on the prevention of ML/TF, avoiding its involvement in operations associated with the preceding type of crime (i.e., the underlying illicit facts from which the advantages to be laundered originate) or leading to the financing of terrorism, according to the result of the risk assessment developed internally and in compliance with the applicable sector regulations.

Additionally, the heads of the Compliance Function/AML Officers and the Employees that perform duties related to ML/TF prevention and compliance with sanctions as well as Audit activities in the Obliged Entities of the CTT Group share with each other all relevant information for the purposes of preventing and combating money laundering and the financing of terrorism. This includes providing information on: (i) customers, accounts and specific operations; and (ii) suspicions that certain funds or other assets are derived from criminal activities or related to the financing of terrorism, provided that there is no opposition from the Financial Intelligence Unit of the Criminal Investigation Police ("FIU").

8.3. General Risks - Use of Cash

In the Summary Report of the National ML/TF Risk Assessment with reference to December 2019, the use of cash was identified as one of the main vulnerabilities of the Financial Sector, so this matter assumes special relevance, and the use of additional control measures (EDD) must be

considered according to the risk identified, as defined in point 9.1.2. Enhanced Due Diligence (EDD).

9. ML/TF Risk Management and Compliance with Sanctions (control duty)

The Obliged Entities of the CTT Group seek to comply with the best international practices in the scope of KYC, KYCC, KYT principles and prevention of ML/TF and compliance with sanctions, within the legal, regulatory and recommendatory frameworks in force.

Accordingly, procedures have been defined regarding ML/TF risk management and compliance with sanctions, with the purpose of promoting high ethical and professional standards and preventing the possibility of the CTT Group Obliged Entities being used for the pursuit of criminal activity. CTT Group entities and their employees are obliged to comply with the preventive duties of ML/TF legally defined and listed in the following points of this Policy.

9.1. Know-Your-Customer Approach ("KYC"/"CDD")

The KYC/CDD strategy translates into an integrated process for accepting new Customers, monitoring Business Relationships and accepting Occasional Transactions, as defined in Law 83/2017 of 18 August, as amended.

Within the scope of the Business Relationships, the KYC/CDD cycle encompasses the procedures for accepting the Business Relationship, continuous monitoring of the Client's information and his/her activity during the term of the relationship. The KYC/CDD cycle ends when the Business Relationship ceases.

Occasional Transactions occurring outside a Business Relationship and not linked to accounts, if applicable, are registered. For this purpose, the identifying elements and transactional data are collected from the Intervening Party(ies) (with the attribution of risk levels and the weighting of additional due diligence measures according to the attributed risk level). In situations classifiable as Business Relationship, the collection of information for registration purposes follows the established KYC/CDD procedures, and upon conclusion of the analysis and assessment process of the counterparty, a low, medium or high level of ML/TF risk is attributed according to the ML/TF risk model defined.

The procedures described aim to obtain data on the Customers of the Obliged Entities of the CTT Group, not only with regard to their identification, but also with regard to the type of financial (or

other) products and services acquired, recurring transactions, origin and destination of funds, and rationale of the transactions, among others. Additionally, information is collected to help understand the purpose of the Business Relationship with these entities, identifying the nature of the relationship established and substantiating it with other information collected.

The Obliged Entities of the CTT Group adopt measures that contribute to the prevention of noncompliance within the scope of KYC/CDD, namely through the development of due diligence processes, following up and monitoring Customers. The information regarding them is periodically reviewed and updated according to the level of risk identified, not exceeding 5 years for low-risk ML/TF customers and one year for high-risk customers (including PEPs and associated entities – Immediate Family Members (IMF), Persons known to be Close Associates of such persons (PREA) and also Political or Public Office Holders (TCPP) [3].

In the processes of establishment of Business Relationships and Occasional Transactions, it is mandatory to collect information that allows the identification of the Customer and/or Beneficial Owner with whom the Obliged Entities of the CTT Group have a relationship.

To ensure the veracity and timeliness of the information obtained, all documentation (hard copy of the original, electronic version with equivalent value or certified copy) necessary to prove the data collected on the Customer, their Proxy or Beneficial Owner must originate from reliable and independent sources, and its authenticity, validity and correspondence with the identity or other identifying elements of the intervening party must be guaranteed according to the means available.

In addition, notwithstanding the aforementioned periodic review deadlines, these may vary depending on changes in circumstances inherent to the customer's characterization, factors that may result in a change in the attributed risk level.

It is also assessed whether the declared Customer and Beneficial Owner qualify as PEP or TCPP. For this purpose, internal lists and lists provided by external entities may be used. It is also verified whether the declared Customer and Beneficial Owner is included in lists of high-risk persons/entities, as defined by each Obliged Entity of the CTT Group.

Through the use of filtering systems, customers[4] are periodically monitored, using internal and external PEP lists and, if applicable, lists of high-risk persons/entities, in order to assess the

[3] In the case of Payshop, when the quality of PEP is inherent to the function, such as in the case of Municipalities, simplified due diligence measures are applied, such as the exception granted by the Bank of Portugal.

[4] In the case of Payshop, for Representatives and Beneficial Owners.

"coincidence" with persons/entities on these lists. Whenever there is an alert and it is confirmed that the Customer belongs to the lists, the EDD process is carried out and other measures/actions deemed appropriate are taken.

9.1.1. Customer Acceptance (duty of identification and diligence)

To establish a Business Relationship with a potential Customer or to carry out any Occasional Transaction, it is strictly necessary and mandatory to perform the identification and due diligence procedures, applying enhanced due diligence (EDD) when the degree of risk of the Customer or the transaction so justifies.

9.1.2. Enhanced Due Diligence ("EDD")

The Obliged Entities of the CTT Group reserve the right to take enhanced due diligence measures when establishing and monitoring Business Relationships and carrying out Occasional Transactions, regardless of whether the Occasional Transaction is carried out through a single transaction or several transactions that appear to be related to each other and present a high risk of ML/TF. The measures adopted by the Obliged Entities of the CTT Group consist of: (i) obtaining additional information on their Customers, representatives or Beneficial Owners; (ii) carrying out additional steps to verify the information obtained; (iii) the intervention of the Compliance Function/AML Officer, or another one to be defined in the absence of the previous one, to authorize the establishment of Business Relationships or the approval of Occasional Transactions; and (iv) the reduction of time intervals to update information, or other applicable measures defined by the sector authorities.

Whenever the Obliged Entities of the CTT Group establish business relationships, carry out occasional transactions, carry out operations or otherwise relate to high risk third parties, they must adopt enhanced, effective and proportionate due diligence measures.

Considering the high risks of ML/TF associated with the issuance, holding or distribution of virtual assets, an activity that is largely unregulated, the Obliged Entities of the CTT Group shall assess the application of EDD measures in respect of business relationships and individual transactions where it is identified that they resulted from the conversion of these assets into fiat currency and intended for or originated by their customers.

9.1.2.1. Risk Relationships

When establishing Business Relationships, the Obliged Entities of the CTT Group adopt enhanced due diligence (EDD) procedures and make the acceptance of Clients falling into one of the following categories, dependent on a decision by the Compliance Function/AML Officer, or another that exercises such responsibilities:

- Politically Exposed Persons, including Immediate Family Members and Persons Known to be Close Associates, residing in national or foreign territory, or Political or Public Office Holders[5];
- Customers or Beneficial Owners that are resident in geographical areas of higher risk[6];
- Customers presenting a high-risk profile of ML/TF, in accordance with the model in force in the Obliged Entity, at each moment in time;
- Clients who are nationals of a third country who request residence or citizenship rights in Portugal in exchange for capital transfers, the acquisition of goods or public debt securities or investment in corporate entities established in Portugal (candidates for the grant of an ARI - Residence Permit for Investment, regardless of whether the ARI was granted at the time of establishment or during the business relationship);
- Others expressly indicated by the BdP or other sectoral authority.

In Occasional Transactions, whenever possible, the Obliged Entities of the CTT Group define objective criteria for the identification of Customers with increased risk, namely covering the following cases:

- Customers involved in transactions reported to the entities foreseen in the applicable legislation, which have seen their suspicions regarding ML/TF confirmed;
- Customers in relation to whom information has been requested by judicial or police entities, within the scope of the Duty of Cooperation;

[5] List of high-level Prominent Public Functions (PPE) drafted in accordance with the sequence defined in article 2(1) (cc) of Law 83/2017, as amended, available (in Portuguese)at the ML/TF Portal (https://portalbcft.pt/sites/default/files/anexos/lista_de_funcoes_publicas_proeminentes_-_ppe_final_2021.pdf. In the case of Payshop, see footnote 3.

[6] As set out on point (3) of Annex III of Law 83/2017, as amended.

- Clients whose known/declared nationality coincides with that of countries identified by the Financial Action Task Force ("FATF") as having strategic weaknesses in terms of ML/TF prevention or considered to be traditionally related to terrorist financing;
- Politically Exposed Persons and Political or Public Office Holders;
- Clients subject to enhanced due diligence measures by express indication of the BdP.

Those Customers will also be subject to compliance with enhanced monitoring and control procedures or other measures applicable in the context of ML/TF.

9.1.2.2. Prohibited Relationships

The Obliged Entities of CTT Group shall not accept as Customers or carry out Occasional Transactions with persons/entities that present risk factors incompatible with the level of risk tolerated by the Obliged Entities of CTT Group.

These risk factors include the following natural or legal persons:

- Those who refuse to submit the information or documentation required by the Obliged Entities of the CTT Group, when establishing a Business Relationship or carrying out an Occasional Transaction (including information on the ownership and control structure of the Customer, the purpose and intended nature of the Business Relationship, or information on the origin and destination of the funds used in the Business Relationship or Occasional Transaction);
- Of whom the information provided is suspected to be false, inappropriate or out of date;
- Who present false identities or fictitious names;
- Whose Beneficial Owner(s) cannot be identified, or if Customers refuse to identify them.
- With residence or domicile in countries, territories and regions with privileged taxation regimes, included in a list approved through applicable legislation or regulation, countries subject to embargoes or other types of sanctions, and countries with strategic deficiencies in the fight against money laundering and terrorist financing.
- On whom there is information disclosed by criminal investigation bodies, in the media, on social networks, or by any other means, from which it can be deduced, with a reasonable degree of certainty, that they may be related to criminal activities, namely those linked to ML/TF (e.g. drug trafficking, organized crime, corruption, among others).

- Who are on sanctions lists defined by countries or international organizations, namely the European Union in accordance with the Common Foreign and Security Policy (CFSP), the Sanctions Committee in accordance with the various Resolutions of the United Nations Security Council (UNSC).

In addition to the situations mentioned above, the Obliged Entities of the CTT Group reserve the right to refuse or terminate relations with Customers, or to refrain from carrying out transactions, whenever they consider that there may be a risk that their services or infrastructures may be used for ML/TF purposes.

Whenever arising from the analysis of ML/TF risks that motivate the adoption of enhanced due diligence measures under the terms of the legal and regulatory provisions in force or in other internally defined situations that result in a potentially high level of risk, such relationships shall be subject to conditional acceptance (subject to scrutiny by the Compliance area/AML Officer of the Obliged Entity of the CTT Group).

9.1.2.3. Simplified Due Diligence ("SDD")

The Obliged Entities of CTT Group define the possibility of establishing Business Relationships or carrying out Occasional Transactions based on simplified due diligence, according to the results of the risk assessment performed by each entity, and after communication to the competent authority, when applicable.

9.2. Analysis and Monitoring

The Obliged Entities of the CTT Group analyse their Customers, relevant counterparties and transactions taking into consideration potential risk factors, and monitor the relationship established over time, keeping track of the Customers, paying special attention to facts that may indicate suspicious operations or behaviour, including proposed or attempted operations. The objective of the controls implemented is to protect these entities from the various risks and to comply with the legal framework and the policies and procedures defined internally, always taking into consideration the risk profile of the customers, products, transactions and distribution channels involved.

9.2.1. Know Your Transactions (KYT)

As part of the ongoing monitoring of the business relationship and, when applicable, of occasional transactions, the analysis and monitoring approach aims to identify and manage the risk of ML/TF, based on a combination of systems, applications or tools that allow:

- Based on the typology of transactions and Customer or Consumer profile, to generate alarms that identify behavioural and/or transactional profiles with ML/TF risk. The alerts are investigated in order to (i) obtain evidence of the rationale, origin and destination of the funds and their conformity (through transaction information or supporting evidence), or (ii) classify the transaction as potentially suspicious.
- Based on information from the behavioural and/or transactional profile, to generate alerts identifying transactions involving high-risk countries, where applicable, in terms of ML/TF, in accordance with the standards defined internally by the Obliged Entities of the CTT Group.
- Based on the monitoring of the business relationship, to identify Customers who should be subject to increased monitoring.
- Based on the use of filtering systems, the monitoring of transactions in real time or with at intervals defined according to the operating reality of the Obliged Entity of the CTT Group, using lists of persons and entities subject to restrictive measures (mandatory minimum lists: lists of sanctions defined by countries or international organizations, namely the European Union according to the CFSP, the Sanctions Committee according to the various UNSC resolutions) in order to compare certain identifying element(s) of the client, beneficiary and detailed information of the transaction with the listed entity(ies), with the transaction processing being blocked for analysis and decision.
- Based on the use of filtering systems, the monitoring of Customers, using the aforementioned lists, in order to assess the "coincidence" with entities included in the lists. Whenever there is an alert and it is confirmed that the Customer has been placed on the Sanctions lists, the respective assets, if applicable, will be immediately blocked and the legally defined procedures will be executed, in line with the requirements related to freezing obligations arising from financial sanctions.[7]

[7] Pursuant to the provisions of Article 23 of Law 97/2017, as amended.

- Based on the information (documentary or otherwise) provided by Customers, monitor its validity, sufficiency and completeness.
- Based on the information and documentation gathered throughout the Business Relationship, assess whether the Customer's head office becomes resident in countries, territories and regions with privileged taxation regimes, countries subject to embargoes or other types of sanctions, and countries with strategic deficiencies in the fight against ML/TF. The maintenance of the Business Relationship is evaluated, according to the risk assessed by the entity.
- Regarding Occasional Transactions (e.g., national and international money orders), based on information extracted from the system, ensure monitoring procedures in several areas, containing: (i) legal entities, including non-profit organizations; (ii) customers of foreign nationality, with special monitoring of transactions carried out by players with nationality corresponding to a country with increased risk in terms of ML/TF; (iii) PEP/Political or Public Office Holder; and (iv) Customers within the scope of a Business Relationship. Based on information on Occasional Transactions, monitor the alerts, which are registered in a specific list, with daily frequency or other as defined by the Obliged Entity of the CTT Group, including high-risk operations, which are analysed daily, in order to confirm the Customer's risk or classify it as false positive. In situations of false positives, the condition generated in the service is changed in the database.

9.2.2. Examination (duty of examination)

The AML Compliance function analyses all potentially suspicious conduct, activities or operations whose identifying features appear or show that they come from criminal activity or are related to the financing of terrorism, taking into account, among other factors, the level of risk of the customers, the characteristics of the transactions, the coherence, consistency and reasonableness of the detail provided by Customers and the suitability and sufficiency of the documentation provided. The analysis considers the elements that characterize suspicion of an operation, namely:

- The nature, purpose, frequency, complexity, unusualness and atypicality of the conduct, activity or operations.
- The apparent absence of an economic objective or lawful purpose associated with the conduct, activity or operations.

- The amounts, origin and destination of the funds moved.
- The place of origin and destination of the operations.
- The means of payment used.
- The nature, the activity, the operating pattern, the economic and financial situation and the profile of the intervening parties.
- The type of transaction, product, corporate structure or legal arrangements that may favour anonymity in particular.

When analysing suspicious transactions, it may also be necessary to adopt enhanced due diligence measures to obtain additional information on Customers, their representatives or Beneficial Owners, as well as on the transaction itself, and to take additional measures to verify the information obtained.

9.2.3. Reporting Suspicious Transactions (duty to report)

Following the analysis of proposed, attempted, ongoing or performed operations, and whenever it is known, suspected or there are sufficient reasons to suspect that certain funds or other assets, regardless of the amount or value involved, may derive from criminal activities or be related to the financing of terrorism, due reporting is immediately made to the Central Department for Investigation and Penal Action of the Public Prosecutor's Office ("DCIAP") and to the Financial Intelligence Unit of the Judiciary Police (FIU), by the Compliance Function /AML Officer of the Obliged Entity of the CTT Group (as per article 43 of Law 83/2017, of 18 August, as amended).

Reporting is done through the channels defined by the recipient authorities, with at least the minimum mandatory information defined by law.

9.2.4. Abstention situations and procedures (duty of abstention)

By decision of the Compliance Function, the Obliged Entities of the CTT Group shall abstain from carrying out transactions whenever they know or suspect that certain funds or other assets, regardless of the amount or value involved, may be associated with criminal activities or related to the financing of terrorism.

Where the Obliged Entity of the CTT Group considers that abstaining from carrying out the transaction is impossible or, after consulting DCIAP and the FIU, is likely to frustrate the

prevention or future investigation of criminal activities from which funds or other assets derive, of money laundering or financing of terrorism, the transactions may be carried out, with the Obliged Entity immediately reporting the information regarding the transactions to DCIAP and the FIU.

Whenever the duty to abstain is exercised (provided for in Article 47 of Law 83/2017, of 18 August, as amended) by decision of the AML Compliance Function, the DCIAP and the FIU are immediately informed as described in subchapter 9.2.3. The FIU must issue a statement within three working days of receipt of the Communication, and transmit the information found to DCIAP. Within the following four working days, DCIAP may determine the temporary suspension of the execution of the operations in relation to which the duty to refrain was, or should be, exercised, notifying the Obliged Entity to that effect.

The transactions reported under the duty to abstain may be carried out (i) when the Obliged Entity of the CTT Group is not notified within seven working days from the communication of the transaction suspected of the temporary suspension decision, or (ii) when it is notified within seven working days of DCIAP's decision not to determine the temporary suspension, and the transactions may be executed immediately.

9.2.5. Refusal Situations and Procedures (duty to refuse)

The Obliged Entities of the CTT Group shall refuse to initiate Business Relationships, carry out Occasional Transactions or perform other operations, when they fall under the situations described in subchapter 9.1.2.2. Prohibited Relationships.

In the case of Customers that refuse to provide identification elements and the respective means of proof envisaged for the identification and verification of their identity, of their representative(s) or of their Beneficial Owner(s) during the Business Relationship or the Occasional Transaction, or refuse to provide information on the purpose and intended nature of the Business Relationship, or information on the origin and destination of the funds used in the Business Relationship or Occasional Transaction, the Obliged Entities of the CTT Group shall terminate the Business Relationship, analyse the possible reasons for not obtaining the elements, means or information and, whenever the respective assumptions are verified, make the communication set forth in subchapter 9. 2.3 Reporting Suspicious Transactions (duty to report).

9.2.6. Collaboration with the Authorities (duty to collaborate)

Whenever requested, the Obliged Entities of the CTT Group, through the AML Compliance Function, promptly and fully cooperate with DCIAP and the FIU, as well as with other judicial and police authorities, sectoral authorities and the Tax and Customs Authority, namely by providing all the information, clarifications, documents and elements requested, in a complete and timely manner.

9.2.7. Non-Disclosure (duty of non-disclosure)

The Obliged Entities of the CTT Group, as well as the members of their corporate bodies, Employees, agents and any other persons acting on behalf and in the interest of the Obliged Entities, may not disclose to the Customer or to third parties:

- that communications to the competent authorities have been, are being or will be made;
- any information related to the referred communications, irrespective of whether such information derives from internal analyses or from requests made by judicial, police or sector authorities;
- that a criminal investigation or enquiry is underway or may be underway, as well as any other investigations, enquiries, investigations, analyses or legal proceedings to be conducted by the authorities referred to in the preceding paragraph;
- any other information or analysis, whether internal or external, whenever it results from the full exercise of the functions conferred by Law 83/2017, as amended, or from the preservation of any investigations, inquests, analyses or legal proceedings and, in general, the prevention, investigation and detection of ML/TF.

The Obliged Entities of the CTT Group limit interaction with the competent authorities during an investigation to the respective AML Compliance Function.

9.3. System of Sanctions and Restrictive Measures

A restrictive measure is a temporary restriction on the exercise of a certain right by means of the imposition of a prohibition or an obligation, approved by the United Nations or by the European Union, which is aimed at achieving at least one of the following objectives:

- The maintenance or restoration of international peace and security;
- The protection of human rights;

- Democracy and the Rule of Law;
- The preservation of national sovereignty and independence and other fundamental interests of the State;
- The prevention and prosecution of terrorism and the proliferation of weapons of mass destruction.

Restrictive measures are categorised into 'targeted' and 'non targeted' measures, the former being directed at certain persons or entities or aimed at restricting trade in specific goods, and the latter applicable to jurisdictions or territories as a whole.[8]

Depending on the objectives pursued, restrictive measures may impose restrictions of a diplomatic, commercial or financial nature, or to the circulation of individuals, including:

i) **Freezing of funds** – action to prevent any move, transfer, alteration, access to, or dealing with funds in any way that would result in any change in their amount, volume, location, ownership, possession, character, destination or other change that would enable the funds to be used, including portfolio management.

ii) **Freezing of economic resources** – action to prevent the moving, transfer, disposal or encumbrance of assets of every kind, whether tangible or intangible, movable or immovable, which are not funds, but may be used to obtain funds, goods or services in any way, including by selling, hiring or mortgaging them.

Thus, the **freezing of funds** and the **freezing of economic resources** may have as their object the prohibition on making financial transactions or entering into new financial commitments or the provision of financial and technical assistance, brokering services and other services related to the activities under prohibition.

iii) **Embargoes** – may be adopted by supranational entities such as the United Nations Security Council and the European Union, as well as by an individual State, in order to restrict trade in certain goods and services (such as weapons and related material, dual use goods or petroleum products) with the embargoed country. This instrument may be used for different reasons, namely political, military, social and economic reasons. The object of embargoes is always countries and never individuals.

[8] See "Best Practices on Enforcement of Restrictive Measures", Banco de Portugal, 2020

9.3.1. Mechanisms implemented

In addition to this Policy, the Obliged Entities of the CTT Group have adopted a set of procedures, which aim to ensure compliance with the sanctions programmes and restrictive measures adopted by the competent entities in this matter.

In order to ensure compliance with the sanctions and restrictive measures programs, under the terms of the applicable legislation, the Obliged Entities of the CTT Group have the adequate means to ensure, in a swift and timely manner, the full detection and understanding of the content of the restrictive measures, in particular and where applicable, of the lists of persons and entities issued or updated under such measures, even if not available in Portuguese, by way of their supply through an external supplier, inclusion in customer and transaction filtering systems, where applicable, as well as by way of the public consultation mechanisms necessary for their application, including electronic subscription to alerts made available by issuing entities (European Union and UN).

In addition to making the lists of persons and entities subject to restrictive measures available on public information sources (the UN website and the Official Journal of the European Union), the BdP also disseminates, through a specific channel defined for this purpose, information on updates to the lists of restrictive measures published by the Ministry of Foreign Affairs and the Ministry of Finance.

The identifying data collected from a Customer, representative and Beneficial Owner are checked against the lists of restrictive measures published by the European Union, in compliance with the Common Foreign and Security Policy ("CFSP"), by the Sanctions Committee in accordance with the various United Nations Security Council Resolutions ("UNSC"), among others that are considered relevant.

The mechanisms implemented in this area are described in points 9.1.2.2 Prohibited Relationships and 9.2 Analysis and Monitoring.

9.3.2. Implementation of Restrictive Measures

The Obliged Entities of the CTT Group shall adopt the means and mechanisms necessary to ensure compliance with the restrictive measures adopted by the United Nations Security

Council[9] or by the European Union[10] for the freezing of assets and economic resources related to terrorism, the proliferation of weapons of mass destruction, and their financing, against designated persons or entities.

The Obliged Entities of the CTT Group shall communicate to the competent national authorities regarding restrictive measures, the Directorate-General for Foreign Policy of the Ministry of Foreign Affairs ("PESC") and the Planning, Strategy, Evaluation and International Relations Office of the Ministry of Finance ("GPEARI") any information in their possession that may facilitate compliance with restrictive measures, and shall inform those authorities whenever they implement a restrictive measure (as per article 23 of Law 97/2017 of 23 August). The Obliged Entities of the CTT Group shall also immediately inform the Attorney General of the Republic and the competent national authorities (PESC and GPEARI) whenever they have news or suspect that an act or omission susceptible of constituting a violation of a restrictive measure has taken place or is in progress.

In the event of restrictive measures that require the freezing of funds and economic resources, the Obliged Entities of the CTT Group shall immediately proceed to freeze the funds and economic resources under their responsibility, if possible, during the course of their activity. In the event of restrictive measures that require prior information and notification of a transfer of funds, the Obliged Entities of the CTT Group shall immediately notify the competent authorities in order to confirm whether the prior authorization measure for the transfer of funds has been approved.

9.4. Record keeping of documents and information (duty of record keeping)

In order to ensure compliance with the legal provisions on document retention periods and conditions, the Obliged Entities of the CTT Group shall keep copies, records or electronic data extracted from all documents obtained within the scope of the identification and due diligence (KYC) procedures, the documentation included in the processes or files related to the Customers, including the commercial correspondence sent, and any documents, records and analyses, of internal or external nature, that evidence the entities' compliance with the procedures (according to the duties set out in Law 83/2017 of 18 August, as amended) for a period of seven years.

[9] Information available on the website https://www.un.org/securitycouncil/.

[10] Information available on the website https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures_en.

The originals, copies, references, or any other durable supports with identical probative force of the supporting documents and records of the transactions shall always be kept, in such a way as to allow the reconstitution of the transactions, for a period of seven years from their execution, even if, in the case of a Business Relationship, the latter has already terminated.

In the documentation archive the following is also ensured:

- Conservation in durable support, with preference for electronic means.
- Archive in conditions that allow the adequate conservation, easy tracking of and immediate access to documents whenever requested by the FIU and by the judicial, police, sectoral authorities and by the Tax and Customs Authority.

In the context of compliance with the duty of record keeping, to the detriment of any prevalence that may emerge from the rules of the General Data Protection Regulation, namely the exercise of the right to erasure, when in doubt between keeping or destroying, the rule of conservation shall be preferred in favour of this Policy.

9.5. Data Protection and Processing

Preventing and combating money laundering and terrorist financing is expressly recognized as an area of protection of important public interest, including with regard to the processing of personal data carried out on the basis of existing legislation.[11]

The sole purpose of processing personal data is the prevention of money laundering and terrorist financing, and the data may not be further processed for any other purposes, including commercial purposes.

The processing of personal data necessary for the fulfilment of ML/TF preventive duties is thus authorized, and any supporting evidence necessary to verify the data requested may also be processed.

9.6. Training (duty to train)

All members of the corporate bodies and Relevant Employees and New Employees of the Obliged Entities of the CTT Group must have adapted knowledge of (i) the obligations arising from legislation and regulation in the scope of ML/TF prevention and compliance with sanctions;

[11] Pursuant to the provisions of article 57 (2) and (3) of Law 83/2017, as amended, as well as of the General Regulation on Data Protection (GDPR) approved at the European Parliament on 27 April 2016 and with mandatory application as of 25 May 2018 in all EU Member States, replacing in Portugal Law 67/98 of 26 October.

(ii) this Policy and the procedures and controls set up by their entity , to the extent applicable; and (iii) the risks associated with the prevention of ML/TF, their role in the prevention and detection of such risks and ability to recognize transactions that may be related to ML/TF and how to act in such situations.

In order to ensure that the referred corporate bodies and Relevant Employees have the aforementioned knowledge and that it is kept up to date, the CTT Group has training contents, appropriate to the financial and non-financial sector and to the functions performed, which are reviewed at least on an annual basis or whenever relevant changes occur in the applicable legislation and regulations.

The training materials and their evaluation, if any, the dates of the training sessions and the attendance records are kept by the training area team under the Talent Management department (Academia CTT).

In the case of Relevant Employees whose functions are directly related to the prevention of ML/TF, training is provided immediately after their admission.

Whenever possible, training on ML/TF prevention is carried out by internal trainers, especially those who are part of the AML Compliance Function of the Obliged Entities of the CTT Group, and the use of external trainers and training content is subject to a favourable opinion from the heads of the AML Compliance Function, after a qualitative assessment regarding competence and experience in the field of ML/TF prevention and compliance with sanctions.

The CTT Group entities ensure training in the scope of ML/TF prevention and the appropriate communication initiatives to foster a solid Compliance culture, with the following actions to be considered:

- Document drawn up annually and subject to the approval of the Board of Directors, setting out the training needs arising from the legal and regulatory impositions on the subject of ML/TF Prevention, the respective objectives, identification of the nature of the employees for whom it is intended and presentation of the existing internal offer, as well as the definition of objectives on this subject for the year in question.

Updated procedures manuals and other technical documentation as a training complement, permanently allowing the clarification of questions that arise during the execution of the operations.

10. Relations with Counterparties

10.1. Financial Counterparties

Prior to the establishment of correspondent banking relationships, or any other relationship deemed relevant with financial Counterparties, the Obliged Entities of the CTT Group ensure a due diligence process that covers:

- The collection of information on the entity that allows understanding the nature of its activity, as well as the identity of its Beneficial Owners and members of the management body;
- The assessment, based on information in the public domain, of its reputation and the quality of the control and supervision mechanisms to which it is subject, including the assurance that the Counterparty is not a Shell Bank;
- The assessment of internal policies, means and procedures aimed at preventing ML/TF and compliance with sanctions, when the identified risk so justifies.

Depending on the criticality and degree of risk attributed to the relationship, the due diligence process may also involve meetings with the heads of the AML Compliance Function of the potential counterparty, or even going to the entity's facilities to verify in loco the ML/TF prevention mechanisms.

All collected elements will be periodically reviewed and updated according to the degree of risk attributed, not exceeding 5 years for low-risk ML/TF counterparties and 1 year for high-risk counterparties (including PEPs)

The acceptance of the relationship with correspondent banks or other financial counterparties is subject to a favourable opinion from the AML Compliance Function, as defined in the internal Manuals of the Obliged Entities of the CTT Group.

10.2. Non-Financial Counterparties

Each Obliged Entity of the CTT Group assesses the exposure to ML/TF risk in the relationships with non-financial Counterparties, defining the level of diligence to be adopted before starting the relationship and during its term.

11. General Definitions

Activities involving virtual assets – any of the following economic activities carried out in the name or on behalf of a client:

i) Exchange services between virtual assets and fiat money;

ii) Exchange services between one or more virtual assets;

iii) Virtual asset transfer services whereby a virtual asset is moved from one address or wallet to another;

iv) Services of safekeeping, or safekeeping and administration of virtual assets or of instruments that enable the control, ownership, storage or transfer of such assets, including private encrypted keys.

AML Officer – person responsible, within the Compliance Department of each Obliged Entity of the CTT Group, for monitoring compliance with the regulatory framework on ML/TF matters, as well as the policies and procedures that ensure the adequacy of the monitoring.

Anti-Money Laundering Officer – person appointed by the financial entity under Article 16 of the Law, who is responsible for ensuring the effective application of policies and procedures and controls adequate for the effective management of money laundering risks to which the financial entity is or may be exposed, and for monitoring compliance with the regulatory framework in this area.

Beneficial Owner – any natural person on whose behalf a transaction or activity is being conducted or who ultimately owns or controls the Customer, as per the provisions of article 2 (1) (h) of Law 83/2017 of 18 August.

Business Relationship – any relationship of a corporate, commercial or professional nature between the Obliged Entities of the CTT Group and their Customers which, at the time of its establishment, is expected to be long-lasting, characterized, namely, by the provision of services or availability of products by the Obliged Entities of the CTT Group to their Customers, in a generally stable and continuous manner over time and irrespective of the number of individual operations that integrate or come to integrate the established relationship framework.

Collective Investment Undertakings – the institutions mentioned in article 2(1)(aa) of the General Framework for Collective Investment Undertakings, approved in annex to Law 16/2015, of 24 February, as well as collective investment undertakings governed by special legislation.

Compliance Function – the Department or other Structure Unit of the Obliged Entities of the CTT Group designated as responsible for ensuring internally the control of compliance with the regulatory framework on the prevention of money laundering and financing of terrorism, under the terms provided for in Law 83/2017 of 18 August [Article 16].

Coordination Committee – the Coordination Committee for Preventing and Combating Money Laundering and Financing of Terrorism Policies.

Counterparty – any natural or legal person, of a corporate or non-corporate nature, with which the Obliged Entities of the CTT Group carry out a financial transaction or establish a contractual relationship, whether lasting or not, that is not considered a Customer. It includes, namely, correspondent Banks, financial service providers (financial intermediaries), counterparties in financial operations (including the sending and receiving of funds), as well as capital market or even suppliers or service providers.

Customer – any natural or legal person or legal arrangement that contacts the Obliged Entities of the CTT Group with the purpose of having a service provided or a product made available to them, through the establishment of a Business Relationship or the execution of an Occasional Transaction.

Durable medium – any physical or electronic support - optical, magnetic or of any other nature that presents a degree of accessibility, durability, reliability, integrity and readability that allows for easy and permanent access to the information, its faithful and complete reproduction and the correct reading of the data contained therein.

Employee – any natural or legal person who, irrespective of the nature of their contractual relationship, participates in the execution of any operations, acts or procedures inherent to the activity carried out by the Obliged Entities of the CTT Group (see also Relevant Employee).

European Supervisory Authorities – these include the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority.

Financial Institution – any of the following entities: i) a company which, not being a credit institution, carries out one or more of the operations mentioned in Annex I to Law 83/2017 as amended, of which it forms an integral part; ii) an insurance company or insurance intermediary, insofar as it carries on business in the life insurance field; iii) an investment firm within the meaning of Article 4(1)(1) of Directive 2014/65/EC of the European Parliament and of the Council of 15 May 2014, extended by Directive 2016/1034/EC of the European Parliament and of the Council of 23 June 2016, on markets in financial instruments; iv) a collective investment undertaking marketing its shares or units.

Financing the proliferation of weapons of mass destruction – the process of concealing or disguising the destination of assets and income (benefits) intended to finance the proliferation of weapons of mass destruction.

Fiat money – banknotes and coins designated as legal tender, scriptural money and electronic money.

Freezing of funds – action to prevent any move, transfer, alteration, use of, or dealing with funds, or access thereto in any way that would result in any change in their amount, volume, location, ownership, possession, character, destination or other change that would enable the funds to be used, including portfolio management.

Freezing of economic resources – action to prevent the moving, transfer, disposal or encumbering of assets of every kind, whether tangible or intangible, movable or immovable, which are not funds, but may be used to obtain funds, goods or services in any way, including by selling, hiring or mortgaging them.

Funds and economic resources– funds correspond to financial assets and benefits of every kind. Economic resources are assets of any kind, whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services.

Goods – any: i) Funds, financial assets, economic resources or other assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, regardless of the way they are acquired, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets, including bank credits, travellers cheques, bank cheques, money orders, bonds, shares, other securities, drafts and letters of credit;

Group – a collection of entities composed of: (i) a legal person or other entity which ultimately exercises control over one or more other legal persons or entities which are part of the group (parent company), its subsidiaries or other entities in which the parent company or the subsidiaries hold a participation, in particular where one or more indicators of control exist; or (ii) other entities linked to each other by a control relationship, in particular where one or more indicators of control exist.

High-risk third countries – countries or jurisdictions identified by reliable sources, such as published mutual evaluation, detailed assessment or monitoring reports (particularly by the FATF), as not having effective systems to prevent and combat money laundering and terrorist financing, without prejudice to the provisions of the Law in respect of high risk third countries.

Immediate family members – i) the spouse or non-marital partner of the politically exposed person; ii) relatives by consanguinity or by affinity in the first degree of the politically exposed person; iii) non-marital partners of the politically exposed person referred to in the previous sub-paragraph, insofar as they do not benefit from the status of affinity; iv) persons who, in other legal systems, occupy similar positions.

Indicators of control – any of the following situations: i) a parent company wholly controls another entity in accordance with sub-paragraph iii and iv ; ii) one entity and one or more other entities, with which the first entity is not related as described in the previous sub-paragraph, are placed under a single management, by virtue of a contract concluded with that first entity or statutory clauses of these other entities; iii) the management or supervisory bodies of an entity and those of one or more other entities, with which the former is not related as described in subparagraph i), are, for the most part, composed of the same persons in office during the financial year in course and until the preparation of the consolidated financial statements; iv) the effective control of an entity is exercised by a limited number of partners and the decisions relating to it result from common agreement between them (situation of joint control).

Know Your Customer (KYC) – expression of Anglo-Saxon origin meaning in-depth knowledge of the Customer, namely through customer due diligence (CDD) activities.

Legal arrangement – separate personal estates, such as condominiums of immovable property in horizontal ownership, trusts under foreign law and similar legal entities, when and in the terms in which their relevance is conferred by domestic law, being considered similar to trusts those legal entities that have, at least, the following characteristics: i) the assets constitute a separate asset

and do not form part of the assets of its trustee; ii) the trustee, or whoever represents the collective entity, figures as the owner of the assets; and iii) the trustee is subject to the obligation to administer, manage or dispose of the assets and, where applicable, to render accounts, in accordance with the rules governing the collective entity.

Money laundering – corresponds to (i) the conduct provided for and punished by Article 368-A of the Criminal Code, (ii) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity, and (iii) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of such actions.

Obliged Entities of the CTT Group – the Entities integrating the CTT Group that, at each moment, are subject to the provisions of Law 83/2017, of 18 August, and other applicable legislation, within the scope of the measures to combat money laundering and the financing of terrorism.

Occasional Transaction – any transaction carried out by the Obliged Entities of the CTT Group outside the scope of an already established Business Relationship, being characterized, namely, by its expected punctuality.

Payment Account – an account held in the name of one or more payment service users, which is used for the execution of payment transactions within the meaning of Article 2(g) of the Legal Framework for Payment Services and Electronic Money ("RJSPME"), annexed to Decree-Law 91/2018 of 12 November.

Persons known to be close associates – i) any natural person known as the co-owner with a politically exposed person of a legal person or legal arrangement; ii) any natural person who is the owner of the share capital or the holder of voting rights of a legal person, or of the property of a legal arrangement, known to have a politically exposed person as its beneficial owner; iii) any natural person known to have a corporate, commercial or professional relationship with a politically exposed person.

Police Authorities – the criminal police bodies competent for the investigation of ML/TF crimes, in accordance with the law, as well as for the investigation of the respective underlying crimes.

Political or Public Office Holder – natural person who, not being qualified as a PEP, holds or has held, in the last twelve months and in the national territory, any of the following positions:

i) the positions listed in Law 52/2019 of 31 July, as amended by:

- Law 69/2020 of 9 November, harmonizing the content of the single declaration of income, assets, interests, incompatibilities and impediments with the respective form,
- Law 58/2021 of 18 August, which introduced changes in the declaratory obligations regarding membership or performance of functions in entities of an associative nature, and also amended Law 52/2019, of 31 July, and the Statute for Members of Parliament;
- Law 4/2022 of 6 January, which extended the declaratory obligations of holders of political offices and senior public positions, amending Law 52/2019, of 31 July;

ii) members of a representative or executive body of a metropolitan area or of other forms of municipal association.

Politically Exposed Person (PEP) – natural person who performs or has performed, in the last twelve months in any country or jurisdiction, any function defined in Article 2(cc) of Law 83/2017, of 18 August as amended.

Relevant Employee - any natural or legal person who, regardless of the nature of their contractual relationship: (i) has responsibility for the characterisation and supervision of processes related to the prevention of ML/TF (including the performance of effectiveness tests); (ii) has responsibility for the execution of processes and procedures covered by the Policy; (iii) performs ML/TF prevention controls; (iv) supports interaction with Clients; or (v) performs relevant operational functions in or for the Obliged Entities of the CTT Group.

Remote means of communication – any means of communication - telephonic, electronic, telematic or other - that enables the establishment of business, the execution of occasional transactions or the performance of operations in general, without the physical or simultaneous presence of the financial entity and its customer.

Representatives – all persons with decision-making powers in the business relationship, including powers to operate accounts on the basis of a legal or voluntary instrument of representation, as well as proxies, business managers or any other natural or legal persons, of any nature, who act before the financial entity on behalf or in the interest of its clients.

Restrictive Measures– temporary restriction on the exercise of a right by means of the imposition of a prohibition or obligation, approved by the United Nations or by the European Union and which seeks to achieve at least one of the following objectives:

a) The maintenance or restoration of international peace and security;

b) The protection of human rights;

c) Democracy and the rule of law;

d) The preservation of national sovereignty and independence and other fundamental interests of the State;

e) The prevention and suppression of terrorism and of the proliferation of weapons of mass destruction.

Sectoral Authorities – these include the following Portuguese authorities: Supervisory Authority for Insurance and Pension Funds (ASF), Banco de Portugal (BdP), Portuguese Securities Market Commission (CMVM), Inspectorate-General for Finance, General Inspection of the Ministry of Work, Solidarity and Social Security, Gaming Regulation and Inspection Service of Turismo de Portugal, I.P., Institute of Public Markets, Real Estate and Construction, I.P. (IMPIC, I.P.) and Food and Economic Security Authority (ASAE).

Senior management – an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

Shell Bank – any entity engaged in its own or equivalent activity to that of a financial entity that is incorporated in a country or jurisdiction in which it has no physical presence, involving meaningful direction and management (a physical presence does not include merely a local agent or junior employees) and is not part of a regulated financial group.

Structure Units – departments, areas, offices or other structures defined and identified in the functional/organisational structure of the Obliged Entities of the CTT Group.

Terrorist financing – the conducts provided for and punishable by article 5 - A of Law 52/2003 of 22 August.

Transfer of funds – any transfer within the meaning of article 3(9) of Regulation (EU) 2015/847.

Virtual asset – digital representation of value which is not necessarily linked to a legally established currency and that does not have the legal status of fiat money but is accepted by natural or legal persons as a medium of exchange or investment and can be transferred, stored and traded electronically.

12. Legal and regulatory references

12.1. International Rules and Recommendations

- Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation, or prosecution of certain criminal offences.
- Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism.
- Council Directive (EU) 2016/2258 of 6 December 2016 as regards access to anti-money-laundering information by tax authorities.
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union.
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds.
- Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries.
- Commission Delegated Regulation (EU) 2018/1108 of 7 May 2018 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regulatory technical standards on the criteria for the appointment of central contact points for electronic money issuers and payment service providers and with rules on their functions.

- Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies.
- FATF Recommendations, particularly i) *Procedures for the FATF AML/CFT/CPF Mutual Evaluations, Follow-Up and ICRG*, ii) *Jurisdictions under Increased Monitoring* and iii) *High-Risk Jurisdictions subject to a Call for Action*.
- G20/OECD Principles of Corporate Governance 2023.
- United Nations Security Council resolution on the application of restrictive measures.
- OECD Guidelines, Chapter VII, 'Combating Bribery and Other Forms of Corruption'.
- Sustainable Development Goals (SDG) 16 – Peace, Justice and Strong Institutions.

12.2. National Rules and Recommendations

- Resolution of the Council of Ministers nº 69/2022 - which approves the "National Strategy for the Prevention and Combat of Money Laundering, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction".
- Law 99-A/2021, of 31 December - Amending several diplomas, including Law 83/2017, of 18 August, which establishes measures to combat money laundering and the financing of terrorism (5th amendment).
- Law 54/2021, of 13 August – Transposes Directive (EU) 2019/1153 on rules aimed at facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.
- Law 58/2020, of 31 August – Transposes Directive (EU) 2018/843 on the prevention of of money laundering or terrorist financing, which amends several laws on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, namely Law 83/2017 and Law 89/2017, also revising Law 97/2017 and the criminal framework provided in Article 368-A of the Criminal Code in which the crime of laundering is typified.
- Law 55/2020, of 27 August – Defines the objectives, priorities and guidelines of criminal policy for the biennium 2020-2022, in compliance with Law 17/2006, of 23 May, which approves the Framework Law on Criminal Policy.

- Law 97/2017, of 23 August – Regulates the application and enforcement of restrictive measures approved by the United Nations (UN) or by the European Union (EU) and establishes the sanctions framework applicable to the violation of these measures.
- Law 92/2017, of 22 August – Compels the use of a specific means of payment in transactions involving amounts equal to or greater than €3,000.
- Law 89/2017, of 21 August, transposes chapter III of Directive (EU) 2015/849 of the European Parliament and of the Council – Approves the Legal Regime of the Central Register of Beneficial Owners.
- Law 83/2017, of 18 August, partially transposes Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015, and Directive (EU) 2016/2258, of the Council of 6 December 2016, amends the Criminal Code and the Industrial Property Code and revokes Law 25/2008 – Establishes measures of a preventive and repressive nature to combat money laundering and the financing of terrorism.
- Law 14/2017, of 3 May, sets out the annual publication of the total value and destination of transfers and remittances of funds to countries, territories and regions with a privileged taxation system.
- Law 52/2003, of 22 August – Act to combat terrorism amended by Laws 57/2007 of 4 September, 25/2008 of 5 June, 17/2011 of 3 May, 60/2015 of 24 June, and 16/2019 of 14 February.
- Law 5/2002, of 11 January and subsequent amendments - Establishes measures to fight organised and economic-financial crime and provides for a special regime of collection of evidence, breach of professional secrecy and loss of assets in favour of the State regarding several types of crime, including ML/TF.
- Decree-Law 91/2018, of 12 November, and Decree-Law 242/2012, of 7 November - Access to the activity of payment institutions/electronic money institutions and provision of payment services/electronic money issuing services.
- Decree-Law 61/2007, of 14 March - Control of cash entering/leaving the European Community through the national territory
- Decree-Law 298/92, of 31 December - General Regime of Credit Institutions and Financial Companies [with particular reference to the provisions of Articles 22(1)(k) (revocation of authorization), 103(2)(e) (acquisition of qualifying holdings), 118-A (refraining from carrying

out and registering operations related to offshore jurisdictions), 165(1)(b) and (c) (deposits excluded from the repayment guarantee) and 167(5) (effectiveness of deposit repayment)].

- Resolution of the Council of Ministers 88/2015, of 6 October – Creates the Coordination Committee for Preventing and Combating ML/TF.
- Ordinance 309-A/2020, of 31 December - Amends Ministerial Order 150/2004, of 13 February, which approves the list of countries, territories and regions with clearly more favourable tax systems.
- Ordinance 200/2019, of 28 June – Establishes the deadlines for the initial declaration of the Central Register of Beneficial Owners, and revokes articles 13 and 17 of Ministerial Order 233/2018.
- Ordinance 310/2018, of 4 December, which regulates the provisions of article 45 of Law 83/2017, of 18 August, defining the types of operations to be reported by the obliged entities to DCIAP and to the FIU.
- Ordinance 233/2018, of 21 August – Regulates the Legal Framework of the Central Register of Beneficial Owners.
- Ordinance 345-A/2016, of 30 December – Establishes the list of countries, territories and regions with privileged taxation systems.
- Ordinance 150/2004, of 13 February – List of countries, territories and regions with privileged taxation systems, amended by Ministerial Order 309-A/2020, of 31 December.
- Order 490/2014 of 23 December 2013 (published in the Official Gazette, 2nd Series, of 10-01-2014) - Determines the establishment of a Working Group to assess the implications of restrictive measures in the internal legal order, identify all regulatory, institutional and operational instruments in force relating to such measures, harmonise these instruments and define the best practices to be followed in the implementation of restrictive measures and reporting mechanisms, and draft the necessary legislative, regulatory and operational amendments.
- Order 9125/2013, of 1 July (published in the Official Gazette, 2nd Series, of 12-07-2013) – Determines the establishment of a Working Group with the objective of carrying out – through the study of the new FATF Standards and the survey of the normative, institutional and operational instruments in force, relating to all matters covered by them – the preparation of

proposals for legislative, regulatory and operational changes, necessary to ensure compliance with those Standards.

- Penal code (article 368-A of which typifies the crime of money laundering).
- Recommendations of the Commission for the Coordination of Policies to Prevent and Combat Money Laundering and the Financing of Terrorism (created by Council of Ministers Resolution 88/2015 of 1 October).

12.3. Sectoral Authorities' Rules and Recommendations

- BdP Notice no. 1/2022, of 6 June - Regulates the conditions of exercise, procedures, instruments, mechanisms, application formalities, reporting obligations and other aspects necessary to ensure compliance with the duties to prevent money laundering and terrorist financing, within the activity of financial entities subject to supervision by Banco de Portugal, as well as the means and mechanisms necessary to ensure compliance with the duties set out in Law 97/2017, and also the measures that payment service providers must adopt to detect funds transfers in which information on the payer or payee is missing or incomplete. Revokes and replaces Notice no. 2/2018 and Instruction no. 2/2021. Article 83(2) of this notice is updated by Notice no. 3/2024 on the deadline for reporting information to the BdP, as well as paragraph 3 of the same article, by repealing subparagraph m).
- BdP Notice no. 2/2021, of 8 April – Defines the regulatory framework applicable to the activity of payment institutions and electronic money institutions, extending to such entities the application, with the necessary adaptations, of BdP Notice 3/2020.
- BdP Notice no. 3/2021, of 13 April – Regulates the registration process with Banco de Portugal of entities wishing to carry out, in Portuguese territory, activities with virtual assets subject to registration, as well as subsequent amendments to the data registered.
- BdP Notice no. 3/2020, of 15 July – Regulates the governance and internal control systems and defines the minimum standards on which the organizational culture of the entities subject to supervision by Banco de Portugal must be based. Revokes Notices nos. 5/2008 and 10/2011, as well as Instruction no. 20/2018.
- BdP Notice no. 8/2016, of 30 September – Duties of registration and communication to the BdP of operations corresponding to payment services whose beneficiary is a natural or legal person based in an offshore jurisdiction (see also BdP Circular Letter No. CC/2016/00000080), of 11 November).

- BdP Notice no. 2/2021, of 8 April – Material scope of the supervision of payment institutions by the Banco de Portugal.
- BdP Notice no. 7/2009, of 16 September – Prohibits the granting of credit to entities based in an offshore jurisdiction considered to be non-cooperative and whose ultimate beneficiary is unknown.
- BdP Instruction no. 25/2020 – Approves the reporting on the activity carried out in national territory by financial entities headquartered in another Member State of the European Union, which operate in Portugal under the freedom to provide services.
- BdP Instruction no. 8/2024 – Defines the specific items of information to be reported annually to Banco de Portugal by the financial entities subject to its supervision in terms of the prevention of money laundering and terrorist financing ('ML/TF'), the respective template and the other terms of submission, in compliance with the provisions of article 83 of Banco de Portugal Notice no. 1/2022, of 6 June. Revokes BdP Instruction no. 5/2019, of 30 January, and BdP Instruction no. 6/2020, of 6 March.
- BdP Circular Letter no. CEX/2022/1000041951, of 6 May 2022 – Amendment to the residence permit for investment ("ARI") and application of enhanced due diligence measures.
- BdP Circular Letter no. CC/2021/00000059, of 10 December 2021 – Risk jurisdictions and strengthening of the FATF list.
- BdP Circular Letter no. CC/2021/00000015 – Use of BPnet for electronic communications and file uploads as part of ML/TF prevention activities.
- BdP Circular Letter no. CC/2021/00000009, of 9 March 2021– Dissemination of Best Practices regarding videoconferencing as an alternative procedure for the proof of identity.
- BdP Circular Letter no. CC/2021/00000003, of 11 January 2021 – Dissemination of Best Practices on the application of restrictive measures.
- BdP Circular Letter no. CC/2020/00000062, of 27 November 2020 – Enforcement of enhanced measures - Use of complex ownership or control structures for money laundering practices.
- BdP Circular Letter no. CEX/2021/1000012261 – Enforcement of enhanced measures – Use of companies established using expedient means to set up companies for money laundering practices, in particular for sending funds of unknown provenance abroad.

- BdP Circular Letter no. CC/2020/00000063, of 27 November 2020 – Enforcement of enhanced measures – Use of companies established using expedient means to set up companies for money laundering practices.
- BdP Circular Letter no. CC/2020/00000055, of 18 September 2020 – Discloses the Form applicable to communications made by payment service providers to Banco de Portugal.
- BdP Circular Letter no. CC/2020/00000035 – Proof of the identifying elements through the means referred to in Article 25(2) of Law 83/2017, of 18 August.
- BdP Circular Letter no. CC/2017/00000018-A – Methodologies for financing the proliferation of WMD.
- BdP Circular Letter no. CC/2017/00000019-A – Indicators of terrorist financing.
- BdP Circular Letter no. CC/2017/00000002 – Enhanced due diligence measures in order to properly manage the increased risks of ML/TF identified in the wake of the "Panama Papers".

13. CTT Group Institutional Information

- **Company name:** CTT – Correios de Portugal, S.A.

  Address: Avenida dos Combatentes, 43, 14th Floor, 1643-001 LISBOA

  SWIFT Code: CTTCPTPL

  Legal nature: Public limited company

  Legal Entity Number (NIPC): 500077568

  Electronic address: www.ctt.pt

  Corporate bodies: www.ctt.pt (Homepage Group CTT > About Us > Corporate Governance > Corporate Bodies)

  Presence abroad: Spain and Mozambique (through companies within the CTT Group)
  Share capital: €69,220,000.00

  Shareholders: holdings in the capital and voting rights of 5 % or more:

  Shareholder structure available at: www.ctt.pt (Homepage Group CTT > Investors > Shareholder Structure

Sectoral Supervising Institutions: BdP – Banco de Portugal (www.bportugal.pt); ASF – Autoridade de Supervisão de Seguros e Fundos de Pensões - Supervisory Authority for insurance and pension funds (www.asf.com.pt)

Statutory Auditor: EY – Ernst & Young

Contact

Address: Avenida dos Combatentes, 43, 14th Floor, 1643-001 LISBOA
Tel.: +351 967 793 578

E-mail: compliance@ctt.pt

Access code for the Permanent Certificate: 1888-1565-6783

- **Company name**: **Payshop (Portugal), S.A.**

Address: Avenida dos Combatentes, nº 43, 14º Piso, 1643-001 LISBOA **SWIFT Code**: n.a.

Legal nature: Public limited company

Legal Entity Number (NIPC): 505231212

Electronic address: www.payshop.pt

Corporate bodies: www.payshop.pt (Homepage Institucional > Quem Somos > Governo da Sociedade > Órgãos da Sociedade)

Presence abroad: n.a.

Share capital: €1,500,000.00.

Shareholders: holdings in the capital and voting rights of 5 % or more: www.payshop.pt (Homepage Institucional > Quem Somos > Governo da Sociedade > Órgãos da Sociedade > Conselho de Administração)

Shareholder structure available at: www.payshop.pt (Homepage Institucional > Quem Somos > Governo da Sociedade > Órgãos da Sociedade > Conselho de Administração)

Sectoral Supervising Institutions: BdP – Banco de Portugal

Statutory Auditor: EY – Ernst & Young and KPMG Advisory – Consultores de Gestão, S.A.

Contact

Avenida dos Combatentes, 43, 14th Floor, 1643-001 LISBOA

Tel.: +351 967 792 640

E-mail: info@payshop.pt

Access code for the Permanent Certificate: 4037-6864-3617