

Regulation No. 4

On Customer Due Diligence of the Entities Carrying Out Financial Activities on a Professional Basis

THE SUPERVISORY AND FINANCIAL INFORMATION AUTHORITY

having regard to the Law No. XVIII on “*Transparency, Supervision and Financial Intelligence*”, of 8 October 2013, and in particular Title II, Chapter III;

whereas:

the Supervisory and Financial Information Authority, on the basis of the risk assessment referred to in Articles 9 and 10 of Law No. XVIII of 8 October 2013, is entrusted with identifying, by regulation, the sectors and typologies of relationships, products, services, operations, transactions and channels of distribution with low risk, pursuant to Article 13 (1) of Law No. XVIII of 8 October 2013;

the Supervisory and Financial Information Authority is entrusted with identifying cases in which simplified and enhanced customer due diligence may be applied and to indicate the procedures and measures to be adopted, including the requirements to be fulfilled, pursuant to Articles 9 (2) (b) (v) (viii), 13 (2), 24 (2) and 25 (2) (3) of Law No. XVIII of 8 October 2013;

the Supervisory and Financial Information Authority is entrusted with supervising and verifying the fulfilment, by the supervised entities, of the obligations established in Title II of Law No. XVIII of 8 October 2013, including Chapter III on customer due diligence, the related obligations established by the regulations, and the guidelines, adopted by the Supervisory and Financial Information Authority itself, pursuant to Article 46 (a) of Law No. XVIII;

the Supervisory and Financial Information Authority is entrusted with sanctioning the violations or systematic non-fulfilment of the obligations established in Title II of Law No. XVIII of 8 October 2013, and related obligations established in the Regulations adopted by the Supervisory and Financial Information Authority itself, pursuant to Article 47 (c) of Law No. XVIII.

In execution of the decision taken by the Board on 20 June 2024

HAS ADOPTED THE FOLLOWING REGULATION

Title I

Area of application, implementation criteria and definitions

Article 1. *Area of application*

This Regulation applies to entities carrying out financial activities on a professional basis.

Article 2. *Implementation criteria*

The provisions of this Regulation shall be applied consistently:

- a) with the institutional, legal, economic, commercial and professional framework of the State;
- b) with the principle of proportionality, taking into account the size and complexity of the operations, the nature of the financial activities carried out, the type of services provided, and the economic and financial framework and effective conditions in which the supervised entities operate.

Article 3. *Definitions*

For the purpose of this Regulation, the following definitions shall apply:

1. «*Suspicious activity*»:

- a) an activity that generates the suspicion or reasonable grounds to suspect that funds or other assets are the proceeds of criminal activities, or are linked or related to terrorism or the proliferation of weapons of mass destruction financing or to be used for terrorism, terrorist acts or by terrorist organizations or those who finance terrorism or proliferation of weapons of mass destruction;
- b) activities, including professional and economic activities, operations or transactions which supervised entities consider particularly likely, by their own nature, to have a link with money laundering or terrorism or proliferation of weapons of mass destruction financing or with terrorist acts or with terrorist organizations or those who finance terrorism or proliferation of weapons of mass destruction.

2. «*Public authority*»: the Curial Institutions and Offices, the Institutions connected with the Holy See or referring to it, included in the list annexed to the Statute of the Council for the Economy, the Governorate of the State and the Judicial Bodies of the State.

3. «*Shell bank*»: a financial institution or a credit institution that has no physical presence in the jurisdiction in which it is incorporated and authorized to carry out its activity and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

4. «*Category and status of the customer*»: classification of customers on the basis of

typology (natural persons, legal persons, etc.) and status (for example: ecclesiastics or lay persons; dignitaries of the Catholic Church; politically exposed persons; etc.); typologies may consist of one or more categories (for example, for natural persons: employees or pensioners of the Holy See or the State; for subjects other than natural persons: Institutes of Consecrated Life and Societies of Apostolic Life; dioceses and parishes of the Catholic Church; non-profit organisations; etc.).

5. «*Correspondent accounts*»: the accounts held by financial institutions, normally on a bilateral basis, for the provision of inter-bank services, like the remittance of drafts, cheques, money orders, transfer of funds, remittance of documents and other transactions.

6. «*Payable-through accounts*»: correspondent accounts that are used directly by third parties on their own behalf.

7. «*Dormant account*»: an account on which no operations or transactions are registered for a period of 10 years.

8. «*Biometric data*»: Personal data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data, which is obtained and processed using technical means.

9. «*Identification data*»:

- a) in the case of natural persons: the first name and surname, the place and date of birth, citizenship, the jurisdiction and the place of residence, and the essential contents of an identity document belonging to the declarant;
- b) in the case of a subject other than a natural person:
 - i) the denomination, the registered office and, if different, the main office;
 - ii) the first name and surname, the place and date of birth, the citizenship, the jurisdiction and the place of residence, and the details of an identity document belonging to the declarant and the indication of his/her role within the legal person.

10. «*Personal data*»: any information relating to an identified or identifiable natural person.

11. «*Delegate*»: a person who acts on a permanent basis in the name and on behalf of the customer on the basis of a legitimately conferred representative mandate.

12. «*Currency*»:

- a) currency, including banknotes and coins that are in circulation as a means of exchange;
- b) bearer negotiable instruments, including monetary instruments in bearer form such as traveller's cheques; negotiable instruments, including cheques, promissory notes and money orders, that are either in bearer form, endorsed without restrictions, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments, including

cheques, promissory notes and money orders, signed, but with the payee's name omitted.

13. «*Identification document*»: an authentic and valid identification document, and in particular:

- a) identity card;
- b) passport (ordinary, service or diplomatic); or
- c) the following documents considered to be equivalent:
 - i) driver's licence;
 - ii) identification cards issued by a public authority of the State;

as long as they are intact, legible, and bear the holder's photograph.

A document is '*authentic*' if it is issued by the competent authority of the Holy See or the issuing jurisdiction.

A document is '*valid*' if the expiry date is later than the date on which it is submitted for the purpose of due diligence.

14. «*Supervised entities*»: entities carrying out a financial activity on a professional basis.

15. «*Family members*»:

- a) the spouse of a politically exposed person;
- b) the children of a politically exposed person and their spouses;
- c) the parents of a politically exposed person.

16. «*Risk factors*»: variables that, either on their own or in combination, may increase or decrease the risk of money laundering and financing of terrorism posed by a relationship or transaction.

17. «*Terrorism financing*»:

- a) the acts set forth in Article 23 of Law No. VIII *on Supplementary norms on criminal law matters*, of 11 July 2013;
- b) participation in acts established by Article 23 of Law No. VIII *on Supplementary norms on criminal law matters*, of 11 July 2013, association to commit such acts, the attempt to perpetrate them, the fact of assisting, instigating or advising someone to commit them or the fact of facilitating their execution;
- c) knowledge, intention or purpose, which must constitute an element of the activities referred to in letters a) and b) may be inferred from objective factual circumstances.

18. «*Funds or other assets*»: any assets, including financial, economic and any other assets, whether tangible or intangible, movable or immovable, however acquired, and any legal documents or instruments, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including bank credits, traveller's cheques, cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

19. «*Jurisdictions at risk*»: Jurisdictions included in the lists published by international or regional bodies, or subject to enhanced monitoring mechanisms by international or regional bodies.

The Supervisory and Financial Information Authority provides the supervised entities with guidelines on the identification of the relevant international or regional bodies.

20. «*Higher-risk jurisdiction*»: the jurisdictions included in the list of high-risk Jurisdictions and in the list of Jurisdictions under increased monitoring, contained in the periodically updated annex to Instruction No. 1 of 28 March 2023 of the Supervisory and Financial Information Authority.

21. «*Third jurisdiction*»: any jurisdiction other than the State.

22. «*Financial Action Task Force*» or «*FATF*»: the international body that sets international standards that aim to prevent money laundering and terrorist and proliferation of weapons of mass destruction financing.

23. «*Person in charge*»: person entrusted to perform specific activities on behalf of the customer according to a clear and unambiguous assignment or mandate.

24. «*Nature and purpose of the relationship*»: classification of the relationship based on its nature (for example, personal account or institutional account) and main purpose declared by the customer (for example, salary crediting, etc.); the categories related to the nature of the relationship may be composed of one or more sub-categories (for example, governmental institutional account, non-governmental institutional account, etc.).

25. «*Remote operations*»: operations carried out when supervised entities provide their services without the physical presence of the customer, the beneficial owner and/or persons acting in the name and on behalf of the customer, and a representative of the supervised entities.

26. «*Occasional operation or transaction*»: a transaction that is not carried out as part of a relationship.

27. «*Non-profit organizations*»: legal persons whose main activity is the collection or distribution of funds or other economic resources for charitable, religious, cultural, educational, social or humanitarian purposes.

28. «*Person who is entrusted with prominent public functions*»:

- a) heads of State or of Government, Ministers and their deputies, Secretaries-General and persons with analogous functions;
- b) members of Parliaments or similar legislative bodies;

- c) members of Supreme Courts, of Constitutional Courts and of other high- level judicial organs whose decisions are not normally subject to appeal, except in extraordinary circumstances;
- d) members of Courts of account and the Boards of Central Banks;
- e) ambassadors and chargés d'affaires;
- f) senior officers of the Armed Forces;
- g) members of management, administration or boards of state-owned corporations;
- h) analogous functions within the Holy See and the State;
- i) members of the governing bodies of political parties;
- j) general secretaries, directors, deputy directors and members of the governance bodies of an international organization.

29. «*Legal person*»: any legal person, whatever the nature and activity, including companies, non-profit organizations and trusts and excluding public authorities.

30. «*Instrumental Legal Person*»: legal person subject to the provisions established in the Apostolic Letter in the form of “*Motu Proprio*” of the Supreme Pontiff Francis on the Instrumental Legal Persons of the Roman Curia, of 5 December 2022.

31. «*Politically exposed person*»: a person who is or has been entrusted with a prominent public function in the Holy See, in the State or in any other jurisdiction or in an international organization. The definition of politically exposed person does not cover middle ranking or more junior officers.

The Supervisory and Financial Information Authority publishes and regularly updates the list of the functions within the Holy See and the State that are qualified as politically exposed persons.

32. «*Payment services provider*»: natural or legal person whose activity includes the provision of payment services or transfer of funds.

33. «*Customer’s risk profile*»: the actual risk to which the customer exposes the supervised entities, defined on the basis of the various risk factors and parameters.

34. «*Relationship*»: relationship of an economic, commercial or professional nature, which may be connected to the activity carried out professionally by obliged subjects and which from the moment of its establishment is presumed to have some duration.

35. «*Correspondent relationship*»:

- a) the provision of financial services by one entity carrying out financial activities on a professional basis, financial institution or credit institutions – correspondent – to another entity carrying out financial activities on a professional basis, financial institution or credit institutions – respondent –, including providing a current or other liability account and related services,

such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;

- b) the relationships between entities carrying out financial activities on a professional basis, financial institutions and credit institutions and among entities carrying out financial activities on a professional basis, financial institutions and credit institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

36. «*Contact details*»:

a) *natural persons*:

- i) address of residence and domicile (if different from the former);
- ii) telephone number and e-mail address, if any;

b) *subjects other than natural persons*:

- i) registered office and main operational office (if different from the former);
- ii) telephone number and e-mail address, if any.

37. «*Money laundering*»:

- a) the acts set forth in article 421*bis* of the Criminal Code;
- b) participation in one of the acts set forth in article 421*bis* of the Criminal Code, association to commit such acts, the attempt to perpetrate them, the fact of assisting, instigating or advising someone to commit them or the fact of facilitating their execution;
- c) knowledge, intention or purpose, which must constitute an element of the activities referred to in letters a) and b) may be inferred from objective factual circumstances.

38. «*Close associates*»:

- a) any natural person who has joint beneficial ownership of a legal person or other close economic relationship with a person belonging to one of the categories established by paragraphs 28 and 31;
- b) any natural person who is the only beneficial owner of a legal person *de facto* created for the benefit of a person belonging to one of the categories established by paragraphs 28 and 31.

39. «*State*»: Vatican City State.

40. «*Beneficial owner*»: the natural person(s) who ultimately owns or controls the entity and/or the natural person(s) on whose name and on whose behalf an operation, transaction or activity is carried out or that is beneficiary of it, and

including at least:

- a) in case of companies:
 - i) the natural person(s) who ultimately owns or controls the legal entity, either through direct or indirect ownership of a sufficient percentage of shares or voting rights or other participation in that entity, including through bearer shares, or through control by other means. A percentage of shares of 25% plus a share or other participation exceeding 25% of the share capital or voting rights of a legal entity held by a natural person constitutes an indication of direct ownership. A percentage of shares amounting to 25% plus a share or other participation exceeding 25% of the share capital or voting rights of a legal entity, held by a legal entity, controlled by one or more natural persons, or by several companies, controlled by the same natural person, constitutes an indication of indirect ownership;
 - ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who holds the position of senior managing official(s) or who exercises in other ways control on directing or managing the company; the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point i) and this point ii), as well as any difficulties encountered in their identification and verification activities;
- b) in the case of a trust or similar legal arrangement, the following persons are included:
 - i) the settlor(s);
 - ii) the trustee(s);
 - iii) the protector(s), if any;
 - iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
 - v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.
- c) in case of non-profit organizations and other subjects other than natural persons:
 - i) the natural person(s) who effectively exercises control of the patrimony of the legal person or entity;
 - ii) if the future beneficiaries have already been established, the natural person(s) who is the effective beneficiary of the patrimony of the legal person or entity;

- iii) if the future beneficiaries of the entity have not yet been determined, the category of persons in whose principal interest the entity has been created or acts;
- iv) if, after all possible means have been exhausted and provided there are no grounds of suspicion, no person has been identified in accordance with the criteria set out in the preceding points, or, in case of doubt as to whether the person or persons identified is or are the beneficial owner(s), the natural person(s) who occupies a senior management position or otherwise exercises control over the direction or management of the entity. The supervised entities are required to maintain records of decisions made in order to the purpose of identifying beneficial ownership, in accordance with points (i), (ii), (iii) and this point (iv), as well as the difficulties encountered in identification and verification.

41. «*Transaction*»:

- a) the transmission or movement of means of payment;
- b) a determined or determinable activity with an economic or financial objective, which modifies the existing juridical situation achieved by a professional performance.

42. «*Linked transaction*»: a transaction which, even if in itself autonomous, constitutes, from an economic perspective, a single operation with one or more operations executed at different stages or moments. For the purposes of this Regulation, transactions effected within a period of 7 days of each other are deemed to be linked, it being understood that a linked transaction exists when there is evidence to suggest that it is so.

43. «*Wire transfer*»: a transaction, typically carried out at least partially by electronic means, in the name and on behalf of an originator, by a payment service provider or by a money or value transfer services provider, for the purpose of placing funds or other economic resources at the disposal of a beneficiary, through a payment service provider or a money or value transfer services provider, regardless of whether the originator and the beneficiary are the same person and that the payment service provider or the money or value transfer services provider of the originator and of the beneficiary are the same.

44. «*Trust*»: a legal relationship established – *inter vivos* or *mortis causa* – by a person, the settlor, in which assets are placed under the control of a trustee in the interest of a beneficiary or for a specific purpose.

45. «*Customer*»: subject to whom the supervised entities offer their services, in accordance with their statutes, regulations or internal policies.

Title II

Risk Based approach

Article 4. *Risk Based approach*

1. Supervised entities modulate the intensity and extent of the customer due diligence requirements according to the level of risk of money laundering, terrorist financing and proliferation of weapons of mass destruction associated with the individual customer, or relationship, or transaction, taking into account also the overall risk assessment of the State and its own particular risk assessment.
2. Supervised entities establish in their own internal procedures the controls and customer due diligence measures they adopt in the context of the relationships, transactions and services, including occasional ones. The internal procedures shall include, as a minimum, what is set out in this Regulation and, in any case, may be amended if requested by the Supervisory and Financial Information Authority.
3. Supervised entities are required to exercise autonomy, independence, and accountability in assessing all potentially relevant risk factors related to the geographical area, customer category, type of relationship, service or product, transaction, and distribution channel.
4. In order to facilitate the assessment by supervised entities, the Supervisory and Financial Information Authority provides the risk factors included in Annex 1, which are, in any case, illustrative and not exhaustive.
5. The risk factors included in Annex 1 are aimed at mitigating the areas of uncertainty related to subjective or discretionary assessments and are aimed at promoting the consistent assessment of risks and the consistent attribution of a risk profile to customers.
6. Risk factors shall be considered for the purposes of assessing the level of risk of money laundering, terrorist financing, and proliferation of weapons of mass destruction financing, assigning a consistent risk profile to the customer, and associating a proportionate level of risk to relationships, operations, or transactions. They do not by themselves constitute indicators of anomalies for the purposes of suspicious activity reporting requirements.

Article 5. *Customer risk profile*

1. Supervised entities are required to assign a risk profile to the customer.
2. The systems adopted to fulfil the obligation set forth in paragraph 1 shall allow for the overall assessment of the documents, data and information acquired for the purpose of customer due diligence and the overall operations carried out, taking into account the relevant risk factors, and shall ensure, among other things, that:
 - a) weighting is not unduly influenced by only one factor;
 - b) the weighting is not distorted by the consideration of over-generalized categories;

- c) a higher level of risk is assigned in case of higher risk factors established by this Regulation and Law No. XVIII of 8 October 2013;
- d) weighting does not lead to a situation where it is impossible to classify a relationship as higher risk or that the majority of relationships are classified as higher risk.

3. Supervised entities shall in any case ensure that the attribution of the risk profile is consistent with a risk-based approach and with the customer's effective knowledge, and allow the fulfilment of the obligations established by the Law No. XVIII of 8 October 2013 and of this Regulation on higher risk situations.

4. Supervised entities may use information and technology systems to automatically assign the risk profile to the customer or to concur in the determination of elements or parts of the risk profile. This is without prejudice to the fact that risk scores automatically generated by IT systems may be adjusted, where necessary.

5. In case supervised entities use IT systems provided by external parties for the risk profile assignment, supervised entities are required to have proper understanding of the system and criteria used for determining the risk profile.

6. The analyses and assessments that determined the assignment of the risk profile to the customer shall be traceable.

Article 6. Updating and amending the customer's risk profile

1. Supervised entities are required to define the frequency of updating the customer's risk profile, consistent with a risk-based approach and the level of risk associated with the individual customer.

2. Supervised entities are still required to immediately update the customer's risk profile when triggering events occur, based on a risk-based approach.

3. Supervised entities shall ensure that changes in the customer's risk profile and related reasons are recorded.

4. Interventions to reduce the risk profile of an individual customer based on an internal proposal shall be limited to exceptional cases, approved by control function on preventing and combating money laundering, terrorist and the proliferation of weapons of mass destruction financing and adequately justified in writing.

5. The control function on preventing and combating money laundering, terrorist and the proliferation of weapons of mass destruction financing shall periodically monitor at an aggregate level, using a risk-based approach, the elements that have led to decreases in the level of risk.

Article 7. Customer's personal form

1. The data and information collected through customer due diligence fulfilments and the execution of operations and transactions represent the overall knowledge that supervised entities have of the customer and shall be summarized in the customer's

personal form.

2. The customer's personal form includes a summary of the following data and information:

- a) category and status;
- b) beneficial owner and any persons acting on behalf of the customer;
- c) economic and financial characteristics;
- d) risk profile;
- e) operations.

3. The customer's personal form shall be made available for consultation and, where appropriate, editing, by those within the supervised entities charged with performing customer due diligence and conducting controls in the area of preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction. Changes to the customer's personal card shall be recorded.

4. Supervised entities shall verify that the operations, transactions, and funds transfers performed by the customer, the beneficial owner, and persons acting on behalf of the customer are consistent with the customer's risk profile and the customer's overall knowledge.

Title III

Customer due diligence

Chapter 1

Area of application, implementation criteria and definitions

Article 8. *Area of application*

1. Supervised entities are required to fulfil customer due diligence in the following cases:

- a) before establishing a relationship;
- b) before executing, as part of an existing relationship, operations, transactions or transfers of funds of an amount equal to or greater than euro 10,000. This threshold is adjustable, according to a risk-based approach and in line with the customer's typical operations;
- c) before executing occasional operations or transactions equal to or above euro 10,000, regardless of the fact that the operation or transaction is executed in a single operation or in several operations which appear to be linked;

- d) before executing an occasional transfer of funds equal to or above euro 1,000.
2. Supervised entities shall, in any case, fulfil the requirements of customer due diligence:
- a) where there is a suspicion of money laundering or the financing of terrorism or of the proliferation of weapons of mass destruction, regardless of an exemption or applicable threshold;
 - b) where there are doubts as to the reliability or adequacy of the data previously obtained for the identification of the customer, of persons acting in the name of and on behalf of the counterpart or of the beneficial owner.
3. Pursuant to Article 5 (1), letter b), of Law No. XVIII of 8 October 2013, it is forbidden to rely on third parties for customer due diligence.

Article 9. Requirements

1. For the purposes of customer due diligence, the supervised entities shall fulfil, *inter alia*, the following requirements:
- a) identify the counterpart and verify his identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, the means for electronic identification, or other remote or electronic identification procedures;
 - b) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person on the basis of documents, data and information obtained from a reliable and independent source;
 - c) identify the beneficial owner and take reasonable measures to verify its identity, using the relevant documents, data and information obtained from a reliable and independent source, such that the supervised entities are satisfied that they know who the beneficial owner is;
 - d) understand and verify if the counterpart is acting in the name and on behalf of other subjects;
 - e) understand, verify and obtain documents, data and information on, the purpose, nature and source of funds of the relationship and operation, transaction or transfer of funds, even occasional, and on the specific characteristics of the customer;
2. Supervised entities should also conduct ongoing customer due diligence throughout the relationship to ensure that:
- a) the transactions being conducted are consistent with the supervised entities' knowledge of the customer, its activities, its risk profile and the source of funds;
 - b) documents, data or information collected is kept up-to-date and relevant.

3. The extent of customer due diligence measures and the periodicity of ongoing due diligence vary in application of a risk-based approach.

4. Where it is not possible to carry out the requirements set forth in paragraphs 1 and 2, it is mandatory to terminate the relationship and it is prohibited to carry out a transaction or operation. In such cases, supervised entities are required to make a suspicious activity report to the Supervisory and Financial Information Authority.

Chapter 2

Ordinary Customer Due Diligence

Section 1

Opening of new relationships and requests for occasional transactions

Article 10. Identification of the customer, delegates and persons in charge where the customer is a natural person

1. Before opening a relationship, supervised entities are required to identify the customer, any delegates and persons in charge, by acquiring, among other things, the following documents, data and information for each individual:

- a) identification data;
- b) contact details;
- c) copy of an identification document;
- d) category, status and activity;
- e) in the case of delegates and persons in charge, appropriate information or documentation to demonstrate the relation with the customer and its duration, if any.

2. Delegations or assignments on a relationship become effective only upon identification of the delegates or persons in charge.

3. Supervised entities are required to carry out the activities referred to in the previous paragraphs, as a general rule, in the presence of the customer.

Article 11. Additional requirements in case the customer is other than a natural person

1. Supervised entities are required to understand and acquire information about the customer's ownership and/or control structure and identify the customer, the beneficial owner, the legal representative (if different from the beneficial owner),

any delegates and persons in charge.

2. Before opening a relationship, supervised entities are required to identify the customer by acquiring, among other things, the following documents, data and information:

- a) identification data and contact details;
- b) copies of documents showing the name, nature and proof of existence, including the date and jurisdiction of foundation;
- c) copies of documents showing the governing bodies of the customer, including but not limited to the names of the individuals performing the functions of management or senior management, and the beneficial owner;
- d) in the case of non-profit organizations, at least the categories of subjects to which the activities are addressed and the geographical areas involved;
- e) in the case of entities such as foundations or legal arrangements, such as trusts, at least the purposes concretely pursued, the beneficiaries and the trustee, and the management methods;
- f) proof of registration in the register of beneficial owners of the relevant jurisdiction, if applicable.

3. Supervised entities are, in addition, required to identify the beneficial owner, any delegates and persons in charge by, among other things, acquiring the following documents, data and information for each person:

- a) identification data;
- b) contact details;
- c) copy of an identification document;
- d) status and activity;
- e) in the case of a beneficial owner and/or legal representative, delegates and person in charge, relevant documentation showing the relation with the customer and, if established, its duration.

4. Delegations or assignments on a relationship become effective only upon identification of the delegates or persons in charge.

5. The identification, as a rule, must be carried out in the presence of the natural person with powers of representation (legal representative) and/or the beneficial owner.

Article 12. *Identification of the beneficial owner*

1. Supervised entities should identify the beneficial owner using the relevant information, such that the supervised entities are satisfied that they know who the beneficial owner is, as established in Article 3 (40).

2. If the analyses reveal the presence of more than one beneficial owner, supervised entities should carry out identification requirements for all beneficial owners.

3. Supervised entities shall keep records of the measures taken as well as any difficulties encountered during the beneficial owner identification procedure.

Article 13. *Verify the identity of customer, delegates, persons in charge, beneficial owner and/or legal representative*

1. Before opening a relationship, supervised entities are required to verify the identity of the customer, any delegates or persons in charge, the beneficial owner and/or legal representative. Supervised entities are also required to verify the documents, data, and information provided by the customer in a reliable manner, according to a risk-based approach.

2. For customers who are natural persons, delegates, persons in charge, beneficial owners, and/or legal representatives, supervised entities are required to ascertain, according to a risk-based approach, the authenticity and validity of the identification document and documentation provided, including verifying the existence and extent of the power to act on behalf of the customer in a reliable manner.

3. In the case of customers other than natural persons, supervised entities are required to conduct, according to a risk-based approach, adequate verifications with reliable sources, including, among others:

- a) *Acta Apostolicae Sedis*;
- b) Pontifical Yearbook;
- c) bulletin of the Holy See Press Office;
- d) registers held by the Governorate of the State;
- e) yearbooks or other official sources of Episcopal Conferences;
- f) repertoire of the International Associations of the Faithful held by the Dicastery for the Laity, the Family and Life;
- g) registers, records and lists made available by the competent foreign public Authorities;
- h) other reliable and independent sources and databases, including those of specialized suppliers.

Article 14. *Acquisition and evaluation of information on the nature and purpose of the relationship*

1. Supervised entities should acquire, evaluate, and understand information on the nature of the activities, in the case of a customer other than a natural person, and the purpose of the relationship.

2. The depth and the scope of the acquisition and evaluation of the information specified in paragraph 1 should be proportionate to the category and status of the customer, according to a risk-based approach.

3. Supervised entities before opening a new relationship are required to acquire, among other things, the following information:

- a) purpose for opening the relationship;
- b) source of funds;
- c) type of services requested;
- d) expected operations, including potential volumes, reason for the opening the relationship, and counterparties;
- e) latest economic situation (e.g., annual income, annual turnover, etc.) and financial situation (e.g., total assets owned) of the customer, including main sources of income;
- f) employment status of the natural person customer, the beneficial owner and/or legal representative and persons appointed to act on behalf of the customer.

4. Part of the information about the nature and purpose of the relationship may also be inferred from the category and status of the customer, or the type of relationship or services requested by the customer, according to a risk-based approach

5. Supervised entities are required to assess the appropriateness and consistency of the information acquired and indicated in paragraphs 3 and 4 above with independent in-depth investigations according to a risk-based approach.

Article 15. *Requirements in the case of occasional operation*

In the case of a request for an occasional operation or transaction, supervised entities are required, according to a risk-based approach, to comply with the same requirements set forth in Articles 10, 11, 12, 13, and 14 (2) (3) (b) (e) (f) (4) (5) and, in any case, to acquire relevant documentation and/or request information useful for assessing, among other things, the purpose and nature of the occasional operation and the destination of the funds, including Jurisdiction and subjects involved.

Article 16. *Doubts about the authenticity of data, information and documents*

1. If there is any doubt about the authenticity of the data, information and documents provided by the customer during customer due diligence, supervised entities are required to take appropriate measures to ascertain their authenticity.

2. For the cases mentioned in paragraph 1, if doubts remain, supervised entities are required to immediately report suspicious activity to the Supervisory and Financial Information Authority and to refuse to open a relationship or carry out an occasional transaction.

Section 2

Operations within an existing relationship

Article 17. *Customer due diligence requirements for operations, transactions, or transfers of funds within an existing relationship*

1. When carrying out operations, transactions, or transfers of funds in the cases set forth in Article 8 (1) (b), supervised entities are required to identify the customer, beneficial owner, and/or legal representative, delegate, or person in charge requesting their execution and verify their identity, through adequate means.
2. In the cases referred to in paragraph 1, supervised entities are required to verify the existence and validity of the power to act on behalf of the customer by the requester of operations, transactions or transfers of funds.
3. Supervised entities should, in addition, assess the nature and purpose of the operation, transaction or transfer of funds, through the acquisition of relevant documentation and/or the request for information useful to assess, among other things, the following issues:
 - a) source of funds, including jurisdiction and subjects involved;
 - b) purpose and nature of the operation, transaction or transfer of funds;
 - c) destination of funds, including jurisdiction and subjects involved.
4. The requirements set forth in Paragraph 3 shall be deemed fulfilled if the supervised entities assess that:
 - a) the customer's personal form, pursuant to Article 7, is updated;
 - b) the operation or transaction is consistent with the customer's risk profile and the supervised entities' overall knowledge of the customer;
 - c) there are no indicators of anomalies, such as to lead to suspicions of money laundering or terrorist financing or proliferation of weapons of mass destruction financing.
5. The transfer of funds shall in all cases be accompanied by the data and information specified in Title II of Regulation No. 2 of 27 November 2023.
6. This is without prejudice to the requirements of Article 16.

Section 3

Ongoing customer due diligence

Article 18. *Ongoing customer due diligence*

1. Supervised entities should conduct ongoing customer due diligence during the

course of the relationship to keep customer data and information up to date and detect potential anomalies.

2. For the purposes of paragraph 1, supervised entities should adopt adequate procedures and measures to:

- a) continuously monitor the relationship, including by monitoring its overall operations, to ensure that these are consistent with the customer's risk profile and the supervised entities' overall knowledge of the customer;
- b) ensure that the documents, data and information collected is kept up-to-date and relevant by undertaking ongoing reviews of existing records, consistent with the periodicity established according to the customer's risk profile;
- c) keep the customer's risk profile up to date;
- d) keep the customer's personal form up to date.

3. Verification that documents, data and information are up-to-date should be carried out, in any case, if a customer's request is such that it results in a potential change in the risk profile of the relationship.

4. For the purposes of paragraph 2, supervised entities must have tools and procedures in place to enable, prior to executing to operations, the timely detection of at least the following:

- a) involvement of designated subjects, in accordance with the requirements of Article 75 et seq. of Law No. XVIII;
- b) involvement of politically exposed persons;
- c) negative press reports about the customer, beneficial owner or subjects acting in the name and on behalf of the customer and, where applicable, the beneficiaries of the transaction; in assessing negative media reports or other information sources, supervised entities shall consider their soundness and reliability based, in particular, on the quality and independence of the information sources and the recurrence of the information;
- d) involvement of higher-risk jurisdictions;
- e) expiration of identification documents and, where applicable, delegates and/or term assignments;
- f) involvement of other higher risk elements identified on the basis of the particular and general risk assessment and/or by the Supervisory and Financial Information Authority, which may take into account the FATF's considerations.

5. In addition to what is indicated in the previous paragraph, supervised entities must have procedures, including automated procedures, that enable the identification of:

- a) unusual or anomalous operations with respect to the customer's risk profile and the supervised entities' overall knowledge of the customer;

- b) particularly complex and/or potentially suspicious patterns of operations.
6. Supervised entities should adopt appropriate policies, procedures and measures related to dormant accounts.

Section 4

Remote operations and relationships

Article 19. *Remote customer due diligence*

1. Supervised entities must adopt and formalize procedures and measures proportionate to risk in order to comply with customer due diligence requirements in the case of remote requests by the customer, the beneficial owner and/or persons acting in the name and on behalf of the customer to open a new relationship, or to carry out a transaction and/or transfer of funds, including occasional ones.
2. The measures referred to in paragraph 1 should ensure that supervised entities, according to a risk-based approach, have real knowledge of the identity of the customer, the beneficial owner, and persons acting on behalf of the customer and avoid the risk of fraud.
3. When a relationship is initiated, established or conducted remotely or an occasional transaction is performed remotely, supervised entities shall assess whether the distance results in an increased risk of money laundering, terrorist financing and/or weapons of mass destruction financing and apply proportionate customer due diligence measures.

Article 20. *Remote request to open a relationship or execute an occasional transaction*

1. In the case of a remote request for a new relationship or an occasional transaction, supervised entities shall carry out the identification requirements set forth in Articles 10, 11, and 12 according to a risk-based approach, through the procedure set forth in Annex 4 or other remote or secure electronic procedures approved and regulated in advance by the Supervisory and Financial Information Authority.
2. The identification referred to in Paragraph 1 is fulfilled when:
 - a) identifying data comes from the attestation of the Pontifical Representation to the jurisdiction where the customer is located;
 - b) the identification data comes from public deeds, or authenticated private deeds, or qualified certificates used for the generation of a digital signature associated with IT documents, in the cases established by the legislation of the State;
 - c) the customer possesses a digital identity with a maximum level of security, as well as a digital identity with a maximum level of security or a certificate for the generation of a digital signature, issued under an electronic identification scheme, in the cases established by the legislation of the State;

- d) the customer has already been identified by the supervised entities in relation to another existing relationship, only if the existing information is up to date, relevant and appropriate with respect to the customer's specific risk profile, as well as the characteristics of the new relationship to be initiated.

3. Supervised entities should verify the data, documents and information acquired in the manner set forth in paragraphs 1 and 2 by taking additional measures than those set forth in Article 13 in the application of a risk-based approach. Measures include, but are not limited to, the following:

- a) the first transfer of funds is made with an account in the customer's name or jointly held with a financial institution that is subject to customer due diligence standards that are aligned with those provided by the State, consistent with its international commitments in this regard;
- b) effective and reliable procedures using biometric data, such as to ensure that such data are sufficiently unique to be unambiguously linked to a single natural person;
- c) telephone feedback recorded through a telephone number listed in public directories or on reliable websites;
- d) other verification procedures that ensure with certainty the identity of the customer, the beneficial owner, and persons acting on behalf of the customer.

4. Remote identification and verification do not exempt from the requirements of assessing the purpose and nature of the relationship or occasional transaction under Articles 14 and 15 according to a risk-based approach.

Article 21. *Request for a remote operation, transaction or transfer of funds within an existing relationship*

1. In the case of a request for a remote operation, transaction or transfer of funds within an existing relationship, supervised entities are required to carry out the identification requirements set forth in Article 17 (1) (2), according to a risk-based approach, by acquiring the customer's request through one of the following methods:

- a) IT systems using strong customer authentication mechanisms established by Chapter 5 of the Supervisory and Financial Information Authority's Regulation No. 3 of 23 May 2018;
- b) fax or mail, with a clear signature, accompanied by a copy of an identity document;
- c) e-mail, accompanied by a copy of an identity document.

2. Supervised entities should verify the data, documents and information collected in accordance with Paragraph 1 (b) and (c) by taking adequate measures according to a risk-based approach. Such measures include but are not limited to the following:

- a) recorded telephone verification using the telephone number registered in the IT system of the supervised entities;

- b) verification by other means than that used in the identification phase referred to in paragraph 1, the address of which is recorded in the IT system of the supervised entities;
 - c) effective and reliable procedures using biometric data, which allow the unique identification of that natural person;
 - d) other verification procedures that provide reasonable confidence as to the identity of the customer, the beneficial owner and persons acting on behalf of the customer.
3. The remote identification and verification referred to in paragraphs 1 and 2 do not exempt from the requirements of Articles 16 and 17 (3) (4) (5).

Chapter 3

Simplified customer due diligence

Article 22. *Area of application*

1. Supervised entities may apply simplified customer due diligence measures in the following cases:

- a) in the case of factors indicative of a low level of risk, as set out in Annex 2;
- b) in case the level of risk assigned under Article 5 is low;
- c) where adequate risk mitigation measures are in place.

2. Simplified customer due diligence shall not apply:

- a) in cases where enhanced or specific customer due diligence requirements are mandatory under Chapters 4 and 5;
- b) in cases where the level of risk assigned under Article 5 is higher;
- c) when there is a suspicion of money laundering, terrorist or proliferation of weapons of mass destruction financing.

3. Where simplified customer due diligence is applied, supervised entities shall ensure that a consistent risk profile is assigned and updated in relation to the customer and that up-to-date knowledge of the customer is maintained. Supervised entities are also required to ensure that the measures taken enable the identification of any factors that may require a potential increase in the level of risk and the implementation of ordinary or enhanced customer due diligence measures.

4. Supervised entities should report annually, as part of the particular risk assessment, the types of simplified customer due diligence measures taken, including aggregated data by customer category, to the Supervisory and Financial Information Authority, which may request their review.

Article 23. Simplified requirements

1. In the cases established in Article 22, supervised entities may implement simplified measures in the phases of identification and verification of the identity of the customer, and the acquisition and assessment of information relating to the nature and purpose of the relationship and the source of funds, or of the operation or transaction, or the transfer of funds.

2. Supervised entities, on the basis of a risk-based approach, may implement, *inter alia*, the following simplified customer due diligence measures.

- a) A smaller amount of information requested directly from the customer:
 - (i) at the identification process (e.g. copies of documents from which the nature and proof of existence of the customer, if the entity is registered in the State, can be acquired by accessing the registers kept at the Governorate of the State or other public registers kept by the competent foreign authorities, if available).
 - (ii) when acquiring and evaluating information on the nature and purpose of the relationship and the source of funds, including potential volumes, counterparts and reasons for operations and for opening the relationship and, as well as the economic and financial situation of the customer (e.g. in the case of an employee or pensioner of the Holy See or the State, some information may be deduced from the type of employment relationship, current or past, unless the person has carried out in the last twelve months additional work, professional or productive activities).
- b) A more contained frequency and depth of monitoring activities during ongoing customer due diligence:
 - (i) relationship monitoring, updating of documents, data and customer information, may be less frequent than ordinary customer due diligence, up to a maximum of 5 years;
 - (ii) monitoring of operations, transactions and transfers of funds may be carried out if they exceed some predetermined thresholds.

Chapter 4

Enhanced customer due diligence

Article 24. Area of application

1. Supervised entities should apply enhanced customer due diligence when any of the following situations occur:

- a) in cases of higher risk indicated in Annex 3, specifically:
 - i) where the customer or the beneficial owner under Article 3 (40) is a politically exposed person, or a member of his or her family or a close associate to a politically exposed person, applying, *inter alia*, the

measures set forth in Article 26;

- ii) in cases of relationships, operations, transactions or transfers of funds with subjects, including financial institutions and credit institutions, directly or indirectly related to Higher Risk Jurisdictions, applying, *inter alia*, the measures set out in Article 27;
 - iii) in cases of transactions that are unusual or incoherent with the customer's risk profile and the supervised entities' overall knowledge of the customer, including unnecessarily complex or illogical patterns, operations, transactions, or transfers of funds;
- b) in cases where the level of risk assigned under Article 5 is higher;
 - c) in cases where the General Risk Assessment or the Particular Risk Assessment shows situations or cases of higher risk;
 - d) in cases where the Supervisory and Financial Information Authority detects other cases for which enhanced customer due diligence measures are required, also taking into account the indications of the FATF.

2. Enhanced customer due diligence measures must be applied in addition to ordinary customer due diligence measures.

3. Supervised entities should report annually, as part of the particular risk assessment, the types of enhanced customer due diligence measures taken, including aggregated data by customer category, to the Supervisory and Financial Information Authority, which may request their review.

Article 25. *Enhanced requirements*

1. In the cases established in Article 24, supervised entities should implement enhanced measures in the phases of identification and verification of the identity of the customer, and in the acquisition and assessment of information relating to the nature and purpose of the relationship and the source of funds, or of the operation or transaction, or the transfer of funds, also occasional.

2. Supervised entities, on the basis of a risk-based approach, should implement, *inter alia*, the following enhanced customer due diligence measures.

- a) Increased amount of information during the identification phase, regarding the identity of the customer, legal representative and/or beneficial owner, and delegates (e.g., through the acquisition of more information concerning reputation and integrity).
- b) Increased amount of information during the assessment of the nature and purpose of the relationship, transactions, operations or transfers of funds, even occasional ones, regarding:
 - (i) the status and activity of the customer, the beneficial owner and the delegates or person in charge;
 - (ii) the nature and purpose of the customer's activity, and the status and

- activities of delegates or persons in charge;
- (iii) the source of funds deposited or moved in the relationship, and if the funds originate from a third party, information on the relationship between the customer and the originator of the funds, the reason for the transfer of the funds, and the consistency of the transfer with the customer's risk profile and the supervised entities' overall knowledge of the customer;
 - (iv) the expected operations, including potential volumes, reasons for the operations and for the relationship, and counterparties;
 - (v) the economic and financial situation of family members and close associates, if the user is a politically exposed person.
- c) Authorization from the General Director, or his delegate, before establishing the relationship, after consultation with the control function on preventing and combating money laundering, terrorist and the proliferation of weapons of mass destruction financing.
 - d) Increased frequency and depth of monitoring activities during ongoing customer due diligence:
 - (i) monitoring of the relationship should be more frequent than ordinary customer due diligence, and should in any case be carried out at least annually, in order to assess any factors that may affect the customer's risk profile;
 - (ii) monitoring and analysis of transactions, operations or transfers of funds should always be carried out when a predetermined threshold is exceeded, which must be lower than that established for ordinary customer due diligence, based on a risk-based approach.

Article 26 – *Specific measures in case of politically exposed persons*

1. Supervised entities should have specific tools and measures to verify in a timely manner whether the customer or the beneficial owner falls within the definitions of Article 3 (28) and (31) by matching the information provided by them with reliable sources.
2. The measures in paragraph 1 must be reapplied periodically, including to existing relationships, in order to identify any changes.
3. Where supervised entities have ascertained that the customer or beneficial owner falls within the definitions of Article 3 (28) and (31), in addition to carrying out the other enhanced customer due diligence requirements, they should:
 - a) obtain the authorization of the General Director, or his delegate, before establishing a relationship and, in the case of an existing relationship, to continue the relationship, after consultation with the control function on preventing and combating money laundering, terrorist and the proliferation of weapons of mass destruction financing.
 - c) establish the source of assets and funds of customers and beneficial owners

identified as politically exposed persons;

- d) conduct ongoing and enhanced monitoring of the relationship;
- e) adopt appropriate procedures and enhanced measures to fulfil the obligations of this Article.

4. When the politically exposed person ceases to hold a prominent public function, supervised entities shall continue to apply these measures for at least 12 months after the politically exposed person has ceased to hold the prominent public function and until such time as they believe, after careful analysis, that such risk has ceased.

5. The requirements in the previous paragraphs also apply to family members and close associates to politically exposed persons.

Article 27 - Relationships and transactions involving higher-risk Jurisdictions

With respect to relationships or transactions involving higher-risk jurisdictions in the list attached to Instruction No. 1 of the Supervisory and Financial Information Authority, supervised entities shall apply enhanced customer due diligence measures, following a risk-based approach, including:

- a) obtaining additional information on the customer and on the beneficial owner;
- b) obtaining additional information on the intended scope and nature of the relationship;
- c) obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner;
- d) obtaining information on the reasons for the intended or performed transactions;
- e) obtaining the authorization of the General Director, or his delegate, before establishing a relationship and, in the case of an existing relationship, to continue the relationship, after consultation with the control function on preventing and combating money laundering, terrorist and the proliferation of weapons of mass destruction financing;
- f) conduct enhanced monitoring of the relationship by increasing the number and frequency of controls applied, and selecting the patterns of transactions that need further examination;
- g) any other measures provided for in Instruction No. 1 of the Supervisory and Financial Information Authority.

Chapter 5

Correspondent relationships with the financial and credit institutions of third jurisdictions

Article 28. Requirements

1. Supervised entities should take specific measures for customer due diligence when entering into correspondent relationships with financial institutions and credit institutions of third jurisdictions, in addition to those ordinarily provided under a risk-based approach.
2. The measures referred to in Paragraph 1 provide that the supervised entities, *inter alia*:
 - a) gather sufficient information on the corresponding financial or credit institution of the third jurisdiction in order to fully understand the nature of its activities and to determine, on the basis of the information available to the public, its reputation and the quality of its supervision including whether it was subject to an investigation or measure in the context of money laundering, financing of terrorism or proliferation of weapons of mass destruction and the eventual outcome of such investigation or measure;
 - b) ascertain that the corresponding financial or credit institution of the third jurisdiction is neither a shell bank nor allows shell banks the use of its accounts;
 - c) evaluate controls relating the prevention and countering of money-laundering and financing of terrorism and the proliferation of weapons of mass destruction applied by the corresponding financial or credit institution of the third jurisdiction;
 - d) obtain the authorisation of the General Director, or his delegate, before establishing a new corresponding account, after consultation with the control function on preventing and combating money laundering, terrorist and the proliferation of weapons of mass destruction financing;
 - e) establish and clearly understand in writing the respective responsibilities of the supervised entities and the corresponding financial or credit institution of the third jurisdiction;
 - f) apply ongoing customer due diligence requirements, using a risk-based approach, to the financial institution or credit institution of a third jurisdiction with which they have relationships.
3. In the case of payable through accounts, the supervised entities shall furthermore ensure that the corresponding financial or credit institution of the third jurisdiction:
 - a) has carried out customer due diligence on the customers who have direct access to those accounts;
 - b) has fulfilled the requirements of customer due diligence, including adequate ongoing customer due diligence and, upon request, is able to supply on a timely

basis data and information obtained following the fulfilment of those requirements.

4. The provision in Paragraph 3 (b) is without prejudice to the provision in Article 5 (1) (b) of Law No. XVIII of 8 October 2013, which prohibits relying on third parties for customer due diligence.

Chapter 6

Completion of Customer Due Diligence and the Duty to Refrain

Article 29. Completion of customer due diligence and the duty to refrain

1. Supervised entities shall complete customer due diligence prior to establishing the relationship or the execution of an operation or transaction, in the cases established in Article 8.

2. When it is not possible to complete the customer due diligence (either with the presence of the customer, or remotely), it is prohibited to open a relationship or to execute any operation or transaction.

3. When it is not possible to complete the ongoing customer due diligence, it is mandatory to close the relationship and to prohibit the execution of any operation or transaction.

4. In the cases indicated at paragraphs 2 and 3, supervised entities shall immediately file a suspicious activity report to the Supervisory and Financial Information Authority.

5. In the case of dormant accounts, in addition to the provision referred to paragraph 4, supervised entities shall consider the specific anomaly indicators established by Regulation No. 5 of 19 September 2018 for the purpose of filing a suspicious activity report.

6. In case there is suspicion of money laundering, financing of terrorism or proliferation of weapons of mass destruction, where the implementation of customer due diligence requirements under Article 8 (2) may reveal such suspicion to the customer, or hinder the prosecution of the beneficiaries of the suspicious operation, transaction or transfer of funds, or in general the activity of the competent authorities, the supervised entities may execute the operation, transaction or transfer of funds and are required to immediately file a suspicious activity report to the Supervisory and Financial Information Authority.

7. In the cases referred to in paragraph 6, supervised entities shall keep records of the reasons that led to the execution of the transaction, operation or transfer of funds, and exhibit them to the Supervisory and Financial Information Authority upon request.

8. In the case of cross-border transportation of cash for an amount equal to or above euro 10,000, supervised entities shall not perform the operation or transaction before the customer presents a copy or fills out the declaration of cross-border transportation of cash pursuant to Title VII of Law No. XVIII of 8 October 2013.

Title IV

Registration and record-keeping

Article 30. *Registration and record-keeping*

1. The supervised entities shall register and keep all documents, data and information obtained for the purposes of customer due diligence, in paper or digital format, for a period of 10 years from the end of the relationship, from the closure of an account, from the performance of a service or from the execution of an occasional operation or transaction, pursuant to Article 38 of Law No. XVIII of 8 October 2013.
2. The documents, data and information to be registered and kept includes the information and documents that have been collected during remote customer due diligence, including the customer's video-identification session and connected audio-video files, images and metadata in electronic format.
3. The requirements referred in previous paragraphs are without prejudice to the additional registration and record-keeping requirements established by Article 38 of Law No. XVIII.

Article 31. *Access of competent authorities*

1. The Supervisory and Financial Information Authority and the judicial authority may request, in specific cases and with motivated decision, the registration and record-keeping established in Article 30 for a period longer than 10 years.
2. The data, documents and information registered according to Article 30 shall remain at the disposal of the competent authorities for the activities of analysis and detailed study, as well as for investigative or judicial activities.

Title V

Final provisions

Article 32. *Reporting suspicious activity*

This Regulation is without prejudice to the provisions of Article 40 (1) of Law No. XVIII on the reporting of suspicious activities and to Regulation No. 5.

Article 33. *Implementation of targeted financial sanctions*

The provisions of this Regulation are without prejudice to the obligations pertaining to the financial measures and other preventive measures concerning subjects who threaten international peace and security as set forth in Articles 75 et seq. of Law No. XVIII.

Article 34. *Administrative sanctions.*

In case of violation or systematic non-fulfilment of the obligations established by this Regulation by supervised entities, the Supervisory and Financial Information Authority shall apply the administrative sanctions provided for in Article 47 of Law No. XVIII of 8 October 2013.

Article 35. *Other references*

For matters not governed by this Regulation, reference should be made to the provisions of the law and regulations into force.

This Regulation will enter into force on the day of its publication on the official website of the Supervisory and Financial Information Authority.

Vatican, 21 June 2024

CARMELO BARBAGALLO
President

Seen

GIUSEPPE SCHLITZER
Director

Annex 1

Risk factors

A. Risk factors associated to the geographic area

Supervised entities shall consider the risk factors associated to the geographical area and the relationship between the customer and the geographic area.

1. Supervised entities shall identify the jurisdiction where the customer:

- a) has the residence or domicile, or registered or operational offices;
- b) mainly performs his activities;
- c) mainly performs or receives transfers of funds;
- d) has significant personal, institutional or professional connections.

Supervised entities shall determine the relative importance of risk factors of each jurisdiction in accordance with the nature and purpose of the relationship.

2. In assessing the risk factors associated to each jurisdiction, supervised entities shall take into account, *inter alia*, the following elements:

- a) where the funds used in the relationship have been generated in a third jurisdiction: the effectiveness of the system for preventing and countering money laundering and financing of terrorism and of the proliferation of weapon of mass destruction, and in particular the criteria for the identification of the predicate offence of money laundering;
- b) where the customer is resident or domiciled, or has the registered or operational office, in a third jurisdiction: the effectiveness of the system for preventing and countering tax offenses;
- c) where funds are received from, or sent to, jurisdictions where groups committing terrorist offences are known to be operating: the extent to which this may give rise to suspicion based on what the supervised entities know about the nature and scope of the relationship;
- d) in the case of correspondence account with third financial institutions: the effectiveness of the supervisory and regulatory system.

B. Risk factors associated to the category of the customer

Supervised entities shall consider the risk factors associated to the category of customer.

1. Supervised entities shall consider, *inter alia*, the risk associated to:

- a) category and status of the customer;

- b) economic and financial characteristics of the customer;
- c) activity of the customer;
- d) behaviour of the customer and its consistency with the nature and purpose of the relationship;
- e) reputation and integrity of the customer.

2. Supervised entities shall monitor constantly the consistency between the products, services, operations or transactions performed or requested by the customer and his category and status, economic and financial characteristics and activity, and behaviour, updating consequently the risk profile of the customer.

B.1. Specific risk factors associated to the category of customer

In assessing the risk factors associated to the category of the customer, supervised entities shall take into account, *inter alia*, the following elements:

- a) in case of natural person:
 - i) whether the customer is a family member or a close associate of a politically exposed person;
 - ii) whether the customer holds a prominent position that might enable her to abuse this position for private gain;
 - iii) whether the customer is not an employee or retiree of a body or entity of the Holy See or the State;
 - iv) whether the customer, in addition to being an employee or retiree of a body or entity of the Holy See or the State, performs or performed additional work, professional or productive activities;
 - v) whether the delegates or the person in charge, in the name and on behalf of the customer, do not have links with the customer to justify the delegation or appointment;
- b) in case of subjects other than natural persons:
 - i) whether the customer has a registered or operational office in a higher-risk jurisdiction;
 - ii) whether the customer is not an entity of the Catholic Church;
 - iii) whether the customer is not registered in the register held by the Governorate of the State;
 - iv) whether the members of the management, or the senior management, or the beneficial owner, are politically exposed persons, or family members or close associates of politically exposed persons;
 - v) whether any members of the management, senior management, or beneficial owners, might have a conflict of interest or abuse their position for private gain;

vi) whether the governance model is unnecessarily complex or illogical or not transparent, without an apparent reason;

vii) whether changes having a negative impact in the control systems of the customer are registered;

viii) whether the delegates or the persons in charge of operating in the name, and on behalf of, the customer, do not have a position in the organizational structure of the customer to justify the delegation or appointment.

ix) whether the customer could be instrumentalized for a fictitious ownership of funds or other assets.

B.2. Specific risk factors associated to the activity of the customer

In assessing the risk factors associated to the activity of the customer, supervised entities shall take into account, *inter alia*, the following elements:

a) whether the customer does not carry out an activity of an institutional nature;

b) whether the customer performs or requests operations or transactions in higher-risk sectors or with counterparts operating in higher-risk sectors (for example, buying or selling metals or precious stones, or coins, or other values, real estate, trading goods or services in relation to cash operations), without an apparent reason.

c) if the customer performs or requests operations or transactions that are unnecessarily complex or illogical, of an unusually high amount, or characterized by anomalous patterns, without an apparent consistency with the nature and purpose of the relationship or the overall knowledge the supervised entities have of the customer;

d) whether, over time, the activity of the customer is not consistent with the information collected by the supervised entity on: status and activity, purpose of the opening of the relationship, source of funds, typology of services requested, expected operations, including potential volumes, reasons for transactions and counterparties.

B.3. Specific risk factors associated to the behaviour of the customer

In assessing the risk factors associated to the behaviour of the customer, supervised entities shall take into account, *inter alia*, the following elements:

a) whether the customer is not cooperative in the identification phase;

b) whether the customer is not able to provide the documents, data and information requested;

c) whether the customer requests unnecessary or unreasonable levels of confidentiality, or is reluctant to provide information on his activity;

d) whether the customer intends to carry out one or more occasional operations or transactions where the establishment of a relationship might make more economic and operational sense.

B.4. Specific risk factors associated to the reputation and integrity of the customer

In assessing the risk factors associated to the reputation and integrity of the customer, supervised entities shall take into account, *inter alia*, the following elements:

- a) the presence of reliable and persistent adverse reports about the customer, or the members of the management, or the senior management or the beneficial owner;
- b) the presence of reliable and systematic negative reports on the honourability of the customer, or that of the members of the management, or the senior management or the beneficial owner;
- c) whether the supervised entity is aware of suspicious activity reports, inquiries or inspections, investigations or judiciary proceedings, involving the customer;
- d) whether the customer, or the members of the management, or the senior management or the beneficial owner, are subject to preventive measures of a personal or real nature.

C. Risk factors associated to the typology of relationship, product or service, operation or transaction

1. In assessing the risk factors associated to the typology or relationship, product or service, operation or transaction, supervised entities shall take into account, *inter alia*, the following elements:

- a) the level of transparency or opaqueness of the product or service, operation or transaction;
- b) the complexity of the product or service, operation or transaction;
- c) the value or size of the product or service, operation or transaction.

2. The following products or services, or factors, may contribute to reducing risk:

- a) a product or service with limited functionality, such as, for example:
 - i) a fixed term with low savings thresholds;
 - ii) benefits that cannot be realized in favour of a third party;
 - iii) benefits are only realizable in the long term or for a specific purpose (such as pension funds);
 - iv) low-value advances on salaries, including ones that are conditional on the purchase of a specific good or service;
- b) a service based on the presence of a current account and which can only be used through the same current account.

3. The following products or services, or factors, may contribute to increasing risk:

- a) a product or service that places no restrictions on amount, cross-border transactions or similar product features;

- b) new products, including new channels of distribution, and the use of new or evolving technologies for new or pre-existing products, without adequate safeguards.
- c) unusually large volume of operations or transactions;
- d) investment products managed discretionally by third parties.

C.1. Specific risk factors associated to the level of transparency or opaqueness of the product or service, operation or transaction

In assessing the risk factors associated to the level of transparency or opaqueness of the product or service, operation or transaction, supervised entities shall take into account, *inter alia*, the following elements:

- a) whether products or services, operations or transactions, allow the customer to remain anonymous, to hide the ownership, origin or destination of the funds;
- b) whether a third party, that is not part of the relationship, has *de facto* the possibility to give instructions on the management of the relationship.

C.2. Specific risk factors associated to the complexity of the product or service, operation or transaction

In assessing the risk factors associated to the complexity of the product or service, operation or transaction, supervised entities shall take into account, *inter alia*, the following elements:

- a) whether the product or service allows transfers by, or in favour of, third parties, of a higher amount than what is normally expected for similar products or services;
- b) whether the product or service is not listed on regulated markets.
- c) whether the operation or transaction involves multiple subjects or jurisdictions.

C.3. Specific risk factors associated to the value or size of the product or service, operation or transaction

In assessing the risk factors associated to the value or size of the product or service, operation or transaction, supervised entities shall take into account, *inter alia*, the following elements:

- a) whether the product or service facilitates or encourages high-value operations or transactions;
- b) whether the transactions are higher than what is reasonable to expect considering the category, status and activity of the customer.

D. Risk factors associated to the channel of distribution

In assessing the risk factors associated to the channel of distribution, operation or

transaction, supervised entities shall take into account, *inter alia*, the following elements:

a) whether the relationship is managed exclusively on a non-face-to-face basis, without any evident reason;

b) whether the management of the relationship by the supervised entities requires in all phases the presence of foreign financial intermediaries.

Annex 2

Factors Indicating Potential Low-Risk Situations

The following factors are considered as indicating a low-risk situation.

A. Geographic area

It is assumed that the following jurisdiction are associated to a low-risk.

- a) the State;
- b) jurisdictions that impose obligations to prevent and counter money laundering and the financing of terrorism and of proliferation of weapon of mass destruction equivalent to those established in the State, pursuant to Article 10 (2) (b) (ix) of Law No. XVIII of 8 October 2013;
- c) jurisdictions that credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, recognize as having effective systems for preventing and countering money laundering, terrorist financing and proliferation of weapons of mass destruction;
- d) jurisdictions that credible sources assess as having a low level of corruption or other criminal activity.

B. Category of the customer

It is assumed that the following categories of customers are associated to a low level of risk.

- a) bodies or entities of the State indicated in the “*Fundamental Law of the Vatican City State*” of 22 February 2001 and in Law No. CCCLXXXIV of 16 July 2002 on the *The Government of the Vatican City State*, and subsequent amendments;
- b) public authorities;
- c) instrumental legal persons;
- d) employees or retirees of bodies or entities of the Holy See or the State, unless the subject performs or performed additional work, professional or productive activities, such as to result in a potential additional source of income.

C. Typology of relationship, product or service, operation or transaction or channels of distribution

It is assumed that the following relationship, product or service, operation or transaction or channel of distribution. are associated to a low risk.

- a) Relationships whose main purpose is the crediting of salary or pension by a body or entity of the Holy See or the State.

- b) Pension or similar scheme that provides retirement benefits to employees, where the scheme rules do not permit the assignment of a member's interest under the scheme.
- c) Advance funds connected to a relationship whose beneficial owner is a subject to whom a low level of risk is assigned.
- d) Individual wealth management linked to a relationship.
- e) Custody and management of portfolio.
- f) Cashier's checks connected to a relationship whose beneficial owner is a subject to whom a low risk is assigned.

Annex 3

Factors Indicating Higher-Risk

A. Geographic area

- a) Higher-risk jurisdictions included in the Annex to Instruction No. 1 *With which is published the list of High-risk Jurisdictions and Jurisdictions under Increased Monitoring* of 28 March 2023, and subsequent amendments.
- b) Jurisdictions included in the list of non-cooperative jurisdictions for tax purposes, including those jurisdictions that have not yet fulfilled their commitments for final exclusion from the list, elaborated by the Council of the European Union.
- c) Jurisdictions that credible sources assess to have a high level of corruption or other criminal activity.
- d) Jurisdictions that finance or support terrorist activities or in which recognized terrorist organizations operate.
- e) Jurisdiction at risk, meaning jurisdictions included in the lists published by international or regional bodies, or subject to enhanced monitoring mechanisms by international or regional bodies.

B. Category of customer

- a) Subjects residing or domiciled, or having a registered or operational office in, a higher-risk jurisdiction.
- b) Subjects included in the list of subjects threatening international peace and security, issued by the President of the Governorate of the State, as well as in the lists of designated subjects issued by the competent organs of the Security Council of the United Nations and of the European Union;
- c) Politically exposed persons, their family members, or close associates.
- d) Subjects not included in the categories of customers authorized to access services provided by the supervised entity receiving a relationship or account by succession or donation.

C. Typology of relationship, product or service, operation or transaction or channels of distribution

- a) Relationships characterized by anomalous profiles or kept with anomalous modes.
- b) Relationships managed exclusively on a non-face-to-face basis, without adequate safeguards.
- c) Relationships with delegates, or persons in charge of operating, with no apparent link with the customer.
- d) Relationships with operations, including incoming or outgoing payments, not justified by the nature and purpose of the relationship, category and status or

otherwise by the overall knowledge that the supervised entities have of the customer.

e) Payments received from a third party with no apparent link with the customer.

f) Schemes, operations or transactions characterized by a significant use of cash, without an apparent reason.

g) New products, including new channels of distribution, and the use of new or evolving technologies for new or pre-existing products, without adequate safeguards.

Annex 4

Video-identification procedure in case of remote customer due diligence

1. Supervised entities shall adopt systems ensuring the encryption of the audio/video communication channel through standardized mechanisms, applications and protocols updated to the latest version, as well as the maximum functionality and accessibility by the customers.
2. Supervised entities shall ensure that the video-identification complies with the following technical requirements:
 - a) the video images must be in colour and allow clear visualization of the interlocutor in terms of brightness, sharpness, contrast, fluidity of the images;
 - b) all images, videos, sounds and data must be captured in a readable format and be of sufficient quality to ensure unambiguous recognition of the customer;
 - c) the audio must be clearly audible, without noticeable distortions or disturbances;
 - d) the audio/video session, which relates to the video images and the audio of the customer, must be carried out in environments without particular disturbing elements.
3. Supervised entities shall ensure that the video-identification process is not considered valid if the quality of the audio/video is particularly poor or is deemed not adequate to allow customer identification, or technical deficiencies or unforeseen interruptions in the connection are detected.
4. Supervised entities shall adopt adequate video identification procedures, which include, *inter alia* the following phases:
 - a) statement by the operator of the supervised entity including his name and surname, and function (if applicable);
 - b) acquisition of customer consent to audio/video recording and its conservation in a secure mode;
 - c) acquisition of all data, information, and documentation required by Articles 10, 11, 12, 13, and 14 of this Regulations, using a risk-based approach;
 - d) attestation by the customer of identification data and contact details as defined in Articles 3 (9) and 3 (36) of this Regulation;
 - e) attestation by the customer that the terms for opening a relationship or performing an occasional operation or transaction are known;
 - f) exposure to the camera device of the identification document (front and back) in such a way as to make it possible to clearly display the photograph of the holder and read the information contained therein (place and date of birth, document number, issue and expiry date, issuing authority);
 - g) certification of the customer's mobile phone number and e-mail through

appropriate procedures that require entering a single-use random code or a link to a universal resource locator specially set up for verification.

5. Remote identification procedures do not in any way exempt supervised entities from the obligations of customer due diligence when opening a relationship or executing an occasional transaction, as well as from the requirements under Articles 15 and 31 of this Regulation.

6. The audio/video session is fully recorded and adequately stored pursuant to Article 29 of this Regulation, and all documents and information should be time-stamped.