BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVO
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

Pursuant to Article 35 paragraph 1, subparagraph 1.1 and Article 65, paragraphs 1 and 2, of Law No. 03/L-209 on the Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No. 77/16 August 2010, Prishtina), amended and supplemented by Law No. 05/L -150 on the Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No. 10/03 April 2017), Article 8, paragraph 1, of Law No. 08/L-304 on Banks, Article 114, of Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Bank Financial Institutions (Official Gazette of the Republic of Kosovo/No. 11/11 May 2012, Prishtina), Article 34 of Law No. 08/L-295 on Crypto-Assets, as well as Article 66, paragraph 2, of Law No. 05/L-096 on the Prevention of Money Laundering and Combating the Financing of Terrorism (Official Gazette of the Republic of Kosovo / no. 18 / 15 June 2016, Prishtina), and Article 24b paragraph 15 of Law Nr. 08/L-333 on Amending and Supplementing the Law No. 05/L-096 on the Prevention of Money Laundering and Combating the Financing of Terrorism,the Board of the Central Bank of the Republic of Kosovo, at its meeting held on November 25, 2025, approved the following:

REGULATION ON INFORMATION THAT MUST ACCOMPANY TRANSFERS OF FUNDS AND CRYPTO-ASSETS

CHAPTER I

GENERAL PROVISIONS

Article 1
Purpose

The purpose of this regulation is to establish rules on information on the payer and the beneficiary that must accompany transfers of funds, in any currency, and on information on the initiator and the beneficiary that must accompany transfers of crypto-assets for the purposes of preventing, identifying and investigating money laundering and terrorist financing, where at least one of the payment service providers or crypto-asset service providers involved in the transfer of funds or crypto-assets is licensed in Kosovo. This regulation also establishes rules on internal policies, procedures and controls to ensure the implementation of AML/CFT measures where at least one of the payment service providers involved in the transfer of funds is licensed in Kosovo.

Article 2
Scope

1. This Regulation applies to payment service providers and their branches licensed in Kosovo, which send or receive transfers of funds in any currency. This Regulation also applies to crypto-asset

transfers executed through crypto-ATMs, where the crypto-asset service provider, or the intermediary crypto-asset service provider, of the originator or the beneficiary is licensed in the country.

2. This regulation does not apply to the services listed in Article 3, paragraphs 1.1 to 1.13 and paragraph 1.15 of the Law on Payment Services.

3. This regulation does not apply to transfers of funds or to transfers of electronic money assets made through a payment card, electronic payment instrument, mobile phone or any other prepaid or postpaid technological device with similar characteristics, provided that the following criteria are met:

   3.1. the card, instrument or device is used only to pay for goods and services;

   3.2. The card, instrument or device number accompanies all transfers resulting from the transaction.

4. Notwithstanding paragraph 3 of this Article, this Regulation shall apply when a payment card, electronic payment instrument, mobile telephone or any other prepaid or postpaid technological device with similar characteristics is used to effect transfers of funds or electronic money tokens between natural persons acting as consumers for purposes other than trade, business or professional activity.

5. This Regulation does not apply to persons who have no other activity than the conversion of paper documents into electronic data and who do so in accordance with a contract with a payment service provider, or to persons who have no other activity than the provision of payment service providers with messaging systems or other support systems for the transfer of funds or with clearing and settlement systems.

6. This regulation does not apply to transfers of funds in cases where one of the following criteria is met:

   6.1. involves the withdrawal of cash by the payer from the payer's own payment account;

   6.2. constitutes a transfer of funds to a public authority as payment for taxes, fines or other charges within the country.

   6.3. the payer and the payee are payment service providers acting on their own behalf;

   6.4. is carried out through the exchange of images of checks.

7. This regulation does not apply to transfers of crypto-assets in cases where one of the following criteria is met:

   7.1. the initiator and the beneficiary are crypto-asset service providers acting on their behalf;

   7.2. The transfer constitutes a “person-to-person” transfer of crypto-assets without the involvement of a crypto-asset service provider.

Article 3
Definitions

1. All terms used in this regulation have the same meaning as the terms defined in Law No. 05/L-096 on the Prevention of Money Laundering and Combating the Financing of Terrorism (hereinafter

referred to as the AML/CFT Law) and Law No. 08/L-333 on amending/supplementing the Law No. 05/L-096 on AML/CFT and Law No. 08/L-328 on Payment Services / or with the following definitions for the purpose of this regulation:

1.1. "**Terrorist Financing**" – means as defined in the applicable AML/CFT legislation.

1.2. "**Money Laundering**" – means as defined in the applicable AML/CFT legislation;

1.3. "**CBK**" – Central Bank of the Republic of Kosovo

1.4. "**FIU-K**" – means the Financial Intelligence Unit of Kosovo

1.5. "**Payer**" - means a person who holds a payment account and authorises the transfer of funds from that payment account or, where there is no payment account, who gives an order to transfer funds;

1.6. "**Beneficiary**" - means a person who is the intended recipient of a transfer of funds or crypto-assets;

1.7. "**Payment Service Provider - PRB**" - means any financial institution licensed, registered or authorized under applicable laws and regulations to provide funds transfer services;

1.8. "**Intermediary payment service provider**" means a PRB that is not the PRB of the payer or the payee and that receives and transmits a transfer of funds on behalf of the PRB of the payer or the payee or another intermediary PRB;

1.9. "**Payment account**" – means an account held in the name of one or more payment service users which is used for the execution of payment transactions;

1.10. "**Funds**" – means banknotes and coins, cash or electronic money;

1.11. "**Funds transfer**" - means any transaction carried out at least partly by electronic means on behalf of a payer through a PRB, with the aim of making funds available to the beneficiary, regardless of whether the payer and the beneficiary are the same persons and regardless of whether the PRB of the payer and that of the beneficiary are one and the same, including:

1.11.1. credit transfer;

1.11.2. direct debit;

1.11.3. money transfer (remittance);

1.11.4. transfer made using a payment card, electronic payment instrument, mobile phone or other prepaid or postpaid electronic device with similar characteristics;

1.12. "**Crypto-asset transfer**" – means any transaction that aims to transfer crypto-assets from one distributed ledger address, crypto-asset account, or other device that allows the storage of crypto-assets to another carried out by at least one crypto-asset service provider acting on behalf of an initiator or a beneficiary, regardless of whether the initiator and the beneficiary are the same person and regardless of whether the crypto-asset service provider of the initiator and the beneficiary is the same;

1.13. "**Group Funds Transfer via File**" - means a group of several individual funds transfers combined for transfer;

1.14. "**Unique transaction identifier**" - means a combination of letters, numbers or symbols defined by the PRB, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, which allows traceability of the transaction back to the payer and the beneficiary;

1.15. "**Person-to-person transfer of crypto-assets**" – means the transfer of crypto-assets without the involvement of any crypto-asset service provider;

1.16. "**Crypto-asset**" - means as defined in the Crypto-assets Law;

1.17. "**Crypto-asset service provider**" – means as defined in paragraph 1.2 of Article 3 of the Regulation on the licensing of crypto-asset service operators;

1.18. "**Intermediary crypto-asset service provider**" – means a crypto-asset service provider that is not the crypto-asset service provider of the originator or beneficiary and that receives and transmits a transfer of crypto-assets of the originator or beneficiary, or of another intermediary crypto-asset service provider;

1.19. "**Crypto ATM**" - means physical or online electronic terminals that enable a crypto-asset service provider to perform, in particular, the activity of transfer services for crypto-assets.

1.20. "**Distributed Ledger Technology (DLT) Address**" – means an alphanumeric code that identifies an address on a network using distributed ledger technology (DLT) or similar technology where cryptoassets can be sent or received;

1.21. "**Crypto-asset account**" – means an account held by a crypto-asset service provider on behalf of one or more natural or legal persons and which can be used to effect crypto-asset transfers;

1.22. "**Self-hosted address**" – means a DLT address that is not associated with:

1.22.1. crypto-asset service provider;

1.22.2. an entity established abroad that provides services similar to those of crypto-asset service providers;

1.23. "**Initiator**" – means a person who maintains a crypto-asset account with a crypto-asset service provider, a distributed ledger technology address or a device that allows the storage of crypto-assets and allows a transfer of crypto-assets from that account, distributed ledger technology address or device, or, where there is no such account, distributed ledger technology address or device, a person who orders or initiates a transfer of crypto-assets;

1.24. "**DLT (Distributed Ledger Technology**)" – means as defined in the Crypto-Assets Law;

1.25. "**Legal Entity Identifier" or "LEI**" – means a unique alphanumeric reference code based on the ISO 17442 standard assigned to a legal entity;

1.26. "**SEPA**" – means the Single Euro Payments Area;

1.27. "**Legal entity identifier**" – means a unique code based on the ISO 17442 standard assigned to a legal entity.

1.28. **"Money transfer (remittance)" –** means a payment service where funds are received from a payer, without opening a payment account in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or another payment service

provider acting on behalf of the payee and/or where these funds are received on behalf of and made available to the payee;

1.29. **"Electronic money token" -**means a type of crypto-asset that aims to maintain a stable value by reference to the value of an official currency;

CHAPTER II
OBLIGATIONS FOR PAYMENT SERVICE PROVIDERS

Subchapter I
Obligations for the payer's payment service providers

Article 4
Information accompanying funds transfers

1. The payer's payment service provider must ensure that the transfer of funds is accompanied by the following information about the payer:

   1.1. the name of the payer;

   1.2. the payer's payment account number;

   1.3. the payer's address including the name of the place, the personal number of the official identification document and the customer identification number or date and place of birth;

   1.4. subject to the existence of the required field in the relevant payment message format, and when provided by the payer to its payment service provider, the payer's current LEI, or in its absence, any equivalent official identifier available.

2. The payer's payment service provider must ensure that the transfer of funds is accompanied by the following information of the beneficiary:

   2.1. the name of the beneficiary;

   2.2. the beneficiary's payment account number;

   2.3. subject to the existence of the required field in the relevant payment message format, and when provided by the initiator to its payment service provider, the current LEI of the beneficiary or, in its absence, any equivalent official identifier available.

3. With the exception of subparagraph 1.2 of paragraph 1, and subparagraph 2.2 of paragraph 2 of this Article, in the case of a transfer that is not made to or from a payment account, the payment service provider of the payer shall ensure that the transfer of funds is accompanied by a unique transaction identifier.

4. Before transferring funds, the payer's payment service provider shall verify the accuracy of the information referred to in paragraph 1 of this Article and, where applicable, in paragraph 3 of this Article, on the basis of documents, data or information obtained from a reliable and independent source.

5. The verification referred to in paragraph 4 of this Article shall be deemed to have been carried out when one of the following applies:

   5.1. The identity of the payer has been verified in accordance with the provisions of customer due diligence as set out in the applicable legislation on AML/CFT and the information obtained on the basis of that verification has been stored in accordance with the provisions of Article 64 of the Law on AML/CFT and the Law on amending/supplementing the Law No. 05/L-096 on AML/CFT.

   5.2. The provisions of paragraph 1.4 of Article 19 of the Law on AML/CFT and the Law on amending and supplementing the Law No. 05/L-096 on AML/CFT apply to the payer.

6. Without prejudice to the exceptions provided for in Articles 5 and 6 of this Regulation, the payment service provider of the payer shall not carry out any transfer of funds before ensuring full compliance with this Article.

Article 5
Domestic fund transfers

1. With the exception of paragraphs 1 and 2 of Article 4 of this Regulation, where all payment service providers involved in the payment chain operating in Kosovo, transfers of funds shall be accompanied by at least the payment account number of both the payer and the payee or, where paragraph 3 of Article 4 of this Regulation applies, the unique transaction identifier.

2. Notwithstanding paragraph 1 of this Article, the payment service provider of the payer shall, within three working days of receiving a request for information from the payment service provider of the payee or from intermediary payment service providers, make available the following:

   2.1. for transfers of funds above EUR 1,000, if these transfers are carried out in a single transaction or in several transactions that appear to be linked, information on the payer or beneficiary in accordance with Article 4 of this Regulation;

   2.2. for transfers of funds not exceeding a value of 1,000 euros that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed a value of 1,000 euros, at least:

      2.2.1. the names of the payer and the beneficiary;

      2.2.2. the payment account numbers of the payer and the payee or, where paragraph 3 of Article 4 of this Regulation applies, the unique transaction identifier.

3. With the exception of paragraph 4 of Article 4 of this Regulation, in the case of transfers of funds referred to in paragraph 2.2 of this Article, the payment service provider of the payer is not required to verify information on the payer, except in cases where the payment service provider of the payer:

   3.1. received the funds to be transferred in cash or anonymous electronic money; or

   3.2. there are reasonable grounds to suspect money laundering or terrorist financing.

Article 6

Transfers of funds abroad

1. In the case of group transfers of funds through a file by a single payer, where the payment service providers of the beneficiaries are abroad, paragraph 1 of Article 4 shall not apply to individual transfers of funds grouped together, provided that the group file contains the information referred to in paragraphs 1, 2 and 3 of Article 4 of this Regulation, that that information has been verified in accordance with paragraphs 4 and 5 of Article 4 of this Regulation, and that the individual transfers bear the payer's payment account number or, where paragraph 3 of Article 4 of this Regulation applies, the unique transaction identifier.
2. By way of derogation from paragraph 1 of Article 4 of this Regulation and, where applicable, without prejudice to the information required in accordance with the CBK Regulation on the determination of requirements for credit transfers and direct debits in euro, funds not exceeding the amount of EUR 1,000 and which do not appear to be linked to other transfers of funds which together with the transfer in question exceed the amount of EUR 1,000, shall be accompanied by at least:
   2.1. names of the payer and the beneficiary
   2.2. the payment account numbers of the payer and the payee or, where paragraph 3 of Article 4 of this Regulation applies, the unique transaction identifier.
3. With the exception of paragraph 4 of Article 4 of this Regulation, the payment service provider of the payer does not need to verify the information on the payer referred to in this paragraph, unless the payment service provider of the payer:
   3.1. received the funds to be transferred in cash or anonymous electronic money; or
   3.2. there are reasonable grounds to suspect money laundering or terrorist financing.

Subchapter II
Obligations for the beneficiary's payment service providers

Article 7
Disclosure of missing information on the payer or beneficiary

1. The payment service provider of the payee shall implement effective procedures to detect whether the fields relating to information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been completed using acceptable characters or inputs in accordance with the conventions of that system.
2. The payment service provider of the payee shall implement effective procedures, including, where appropriate, monitoring after or during transfers of funds, in order to detect whether the following information about the payer or the payee is missing:
   2.1. for transfers of funds where the payment service provider of the payer is established domestically, the information referred to in Article 5 of this Regulation;

2.2. for transfers of funds where the payer's payment service provider is abroad, the information referred to in subparagraphs 1.1, 1.2 and 1.3 of paragraph 1 of Article 4 of this Regulation, and in subparagraphs 2.1 and 2.2 of paragraph 2 of Article 4 of this Regulation;

2.3. for group funds transfers through a file where the payer's payment service provider is located abroad, the information referred to in subparagraphs 1.1, 1.2 and 1.3 of paragraph 1 of Article 4 of this Regulation, and in subparagraphs 2.1 and 2.2 of paragraph 2 of Article 4 of this Regulation.

3. In the case of transfers of funds exceeding EUR 1,000, whether such transfers are carried out as a single transaction or in several transactions which appear to be linked, before crediting the payee's payment account or making the funds available to the payee, the payee's payment service provider shall verify the accuracy of the information on the payee referred to in paragraph 2 of this Article on the basis of documents, data or information obtained from a reliable and independent source, as well as whether it is regulated by national legislation without prejudice to the requirements laid down in relation to the time of execution and the date of validity of the transaction.

4. In the case of transfers of funds not exceeding EUR 1,000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed the amount of EUR 1,000, the payment service provider of the payee does not need to verify the accuracy of the information on the payee, unless:

4.1. affects the payment of funds in cash or anonymous electronic money; or

4.2. there are reasonable grounds to suspect money laundering and terrorist financing.

5. The verification referred to in paragraphs 3 and 4 of this Article shall be considered completed when one of the following applies:

5.1. The identity of the beneficiary has been verified in accordance with the provisions of customer due diligence as set out in the applicable legislation on AML/CFT and the information obtained on the basis of that verification has been stored in accordance with the provisions of Article 64 of the Law on AML/CFT and the Law on amending/supplementing the Law No. 05/L-096 on AML/CFT.

5.2. The provisions of paragraph 1.4 of Article 19 of the Law on AML/CFT and the Law on amending and supplementing the Law No. 05/L-096 on AMLCFT apply to beneficiaries.

Article 8
Funds transfers with missing or incomplete information on the payer or beneficiary

1. The payment service provider of the payee must implement effective risk-based procedures, including procedures based on the risk-sensitive element, to determine whether to execute, refuse or suspend a transfer of funds without the complete required information of the payer and the payee and to take appropriate follow-up action.

1.1. Where the payment service provider of the payee becomes aware, when accepting a transfer of funds, that the information referred to in subparagraphs 1.1, 1.2 and 1.3 of paragraph 1 and subparagraphs 2.1 and 2.2 of paragraph 2 of Article 4 of this Regulation, paragraph 1 of Article 5, and Article 6 of this Regulation is missing or incomplete or has not been completed using

characters or inputs acceptable in accordance with the conventions of the messaging or payment and settlement system as referred to in paragraph 1 of Article 7 of this Regulation, the payment service provider of the payee shall, on a risk-sensitive basis:

1.1.1. refuse the transfer of funds; or

1.1.2. request the required information about the payer and the beneficiary before or after crediting the beneficiary's payment account or making funds available to the beneficiary.

2. Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the payment service provider of the payee must:

2.1. take steps, which may initially include issuing warnings and setting time limits, before proceeding with refusal, restriction or termination in accordance with subparagraph 2.2 of this Article if the requested information has not yet been provided; or

2.2. directly refuse any future transfer of funds from that payment service provider or restrict or terminate its business relationship with that payment service provider.

3. Based on the previous paragraph, the beneficiary's payment service provider must report this failure, and the steps taken, to the CBK and the FIU-K.

Article 9
Assessment and Reporting for Beneficiary Payment Service Providers

The payment service provider of the payee must consider missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it should be reported to the FIU-K in accordance with applicable AML/CFT legislation.

Subchapter III
Obligations for intermediary payment service providers

Article 10
Storage of information on the payer and beneficiary accompanying the transfer

Intermediary payment service providers must ensure that all information received about the payer and the beneficiary accompanying a transfer of funds is stored with the transfer.

Article 11
Disclosure of missing information on the payer or beneficiary

1. The intermediary payment service provider must implement effective procedures to detect whether the fields relating to information on the payer and the beneficiary in the messaging or payment and

settlement system used to effect the transfer of funds have been completed using acceptable characters or inputs in accordance with the conventions of that system.

2. The intermediary payment service provider must implement effective procedures, including, where appropriate, monitoring after or during the transfer of funds, to detect whether the following information about the payer or the payee is missing:

   2.1. for transfers of funds where the payment service providers of the payer and the payee are located within the country, the information referred to in Article 5 of this Regulation;

   2.2. for transfers of funds where the payment service provider of the payer or the payee is established abroad, the information referred to in subparagraphs 1.1, 1.2 and 1.3 of paragraph 1, and in subparagraphs 2.1 and 2.2 of paragraph 2 of Article 4 of this Regulation;

   2.3. for group funds transfers through a file where the payer's payment service provider is located abroad, the information referred to in subparagraphs 1.1, 1.2 and 1.3 of paragraph 1, and in subparagraphs 2.1 and 2.2 of paragraph 2 of Article 4 of this Regulation.

Article 12
Funds transfers with missing information on the payer or beneficiary

1. The intermediary payment service provider must establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds that lacks the required payer and payee information and for taking appropriate follow-up measures.

2. Where the intermediary payment service provider becomes aware, when accepting a transfer of funds, that the information referred to in subparagraphs 1.1, 1.2 and 1.3 of paragraph 1 and subparagraphs 2.1 and 2.2 of paragraph 2 of Article 4 of this Regulation, paragraph 1 of Article 5, or Article 6 of this Regulation is missing or incomplete or has not been completed using acceptable characters or inputs in accordance with the conventions of the messaging or payment and settlement system as referred to in paragraph 1 of Article 7 of this Regulation, the intermediary payment service provider shall, on a risk-sensitive basis:

   2.1. refuse the transfer;

   2.2. request information on the payer and beneficiary before or after the transmission of the funds transfer.

3. Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the intermediary payment service provider must:

   3.1. take steps, which may initially include issuing warnings and setting time limits, before proceeding with refusal, restriction or termination in accordance with subparagraph 3.2 of this Article if the requested information has not yet been provided; or

   3.2. directly refuse any future transfer of funds from that payment service provider or restrict or terminate its business relationship with that payment service provider.

   3.3. Based on the previous paragraph, the intermediary payment service provider must report this failure to the CBK and the FIU-K, and the steps taken.

Article 13
Assessment and Reporting for Intermediary Payment Service Providers

The intermediary payment service provider must consider missing or incomplete information on the payer or beneficiary as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it should be reported to the FIU-K in accordance with applicable AML/CFT legislation.

CHAPTER III
OBLIGATIONS FOR CRYPTO-ASSETS SERVICE PROVIDERS

Subchapter I
Obligations for initiator crypto-asset service providers

Article 14
Information accompanying crypto-asset transfers

1. The initiator's crypto-asset service provider must ensure that the crypto-asset transfer is accompanied by the following initiator information:
   1.1. the name of the initiator;
   1.2. the address of the initiator's distributed ledger, in cases where a crypto-asset transfer is recorded on a network using DLT or similar technology, and the initiator's crypto-asset account number, where such an account exists and is used to process the transaction;
   1.3. the initiator's crypto-asset account number, in cases where a crypto-asset transfer is not registered on a network using DLT or similar technology;
   1.4. the address of the initiator including the name of the place, the personal number of the official identification document and the customer identification number or alternatively the date and place of birth of the initiator;
   1.5. subject to the existence of the required field in the relevant message format, and when provided by the initiator to its crypto-asset service provider, the current LEI or, in its absence, any other equivalent official identifier available of the initiator.
2. The initiator's crypto-asset service provider must ensure that the crypto-asset transfer is accompanied by the following beneficiary information:
   2.1. the name of the beneficiary;
   2.2. the address of the beneficiary's distributed ledger, in cases where a crypto-asset transfer is recorded on a network using DLT or similar technology, and the beneficiary's crypto-asset account number, where such an account exists and is used to process the transaction;
   2.3. the beneficiary's crypto-asset account number, in cases where a crypto-asset transfer is not registered on a network using DLT or similar technology;

2.4. subject to the existence of the required field in the relevant message format, and when provided by the initiator to its crypto-asset service provider, the current LEI or, in its absence, any other equivalent official identifier available of the beneficiary.

3. With the exception of subparagraph 1.3 of paragraph 1, and subparagraph 2.3 of paragraph 2 of this Article, in the case of a transfer of crypto-assets that are not registered on a network using DLT or similar technologies and that are not made to or from a crypto-asset account, the initiator's crypto-asset service provider must ensure that the transfer of crypto-assets is accompanied by a unique transaction identifier.

4. The information referred to in paragraphs 1 and 2 of this article must be submitted prior to, or simultaneously or in parallel with, the transfer of crypto-assets and in a secure manner and in accordance with the provisions of the law on the protection of personal data.

5. The information referred to in paragraphs 1 and 2 does not necessarily have to be directly attached to, or included in, the transfer of crypto-assets.

6. In the case of a transfer of crypto-assets made to a self-hosted address, the initiator's crypto-asset service provider must obtain and maintain the information specified in paragraphs 1 and 2 of this article and must ensure that the transfer of crypto-assets is individually identifiable.

7. Without prejudice to the specific risk mitigation measures set out in the applicable AML/CFT legislation, in the case of a transfer exceeding the amount of EUR 1,000 to a self-hosted address, the initiator's crypto-asset service provider must take appropriate measures to assess whether that address is owned or controlled by the initiator.

8. Before transferring crypto-assets, the crypto-asset service provider must verify the accuracy of the information referred to in paragraph 1 of this article on the basis of documents, data or information obtained from a reliable and independent source.

9. The verification referred to in paragraph 8 of this Article shall be deemed to have been carried out when one of the following applies:

   9.1. the identity of the initiator has been verified in accordance with the provisions of customer due diligence as set out in the applicable legislation on AML/CFT and the information obtained on the basis of that verification has been stored in accordance with the provisions of Article 64 of the Law on AML/CFT and the Law on amending/supplementing the Law No. 05/L-096 on AML/CFT;

   9.2. The provisions of paragraph 1.4 of Article 19 of the Law on AML/CFT and the Law on amending and suplementing the Law No. 05/L-096 on AML/CFT apply to the initiator.

10. The initiator's crypto-asset service provider shall not allow the initiation or execution of any crypto-asset transfer before ensuring full compliance with this article.

Article 15
Transfer crypto assets to a group via file

In the case of group transfers of crypto-assets through a file by a single initiator, Article 14 of this Regulation shall not apply to the individual transfers included together therein, provided that the group transfer through the file contains the information referred to in paragraphs 1, 2 and 3 of Article 14 of

this Regulation, that this information has been verified in accordance with paragraphs 6 and 7 of Article 14 of this Regulation and that the individual transfers contain the address of the distributed registry where paragraph 2.2 of Article 14 of this Regulation applies, the crypto-asset account number of the initiator where paragraph 2.3 of Article 14 of this Regulation applies or the unique transaction identifier where paragraph 3 of Article 14 of this Regulation applies.

Subchapter II
Obligations for beneficiary crypto-asset service providers

Article 16
Disclosure of missing information on the initiator or beneficiary

1. The crypto-asset service provider of the beneficiary shall implement effective procedures, including, where appropriate, monitoring after or during transfers, in order to detect whether the information specified in paragraphs 1 and 2 of Article 14 of this Regulation on the initiator and the beneficiary is included in, or follows, the transfer or transfer of crypto-assets through the group file.
2. In the case of a transfer of crypto-assets made from a self-hosted address, the crypto-asset service provider of the beneficiary must obtain and retain the information referred to in paragraphs 1 and 2 of Article 14 of this Regulation and must ensure that the transfer of crypto-assets can be individually identified.
3. Without prejudice to the specific risk mitigation measures set out in the applicable AML/CFT legislation, in the case of a transfer exceeding the amount of EUR 1,000 from a self-hosted address, the beneficiary's crypto-asset service provider must take adequate measures to assess whether that address is owned or controlled by the beneficiary.
4. Before crypto-assets are made available to the beneficiary, the crypto-asset service provider of the beneficiary must verify the accuracy of the information on the beneficiary referred to in paragraph 2 of Article 14 of this Regulation on the basis of documents, data or information obtained from a reliable and independent source.
5. The verification referred to in paragraphs 2, 3 and 4 of this Article shall be considered completed when one of the following applies:
   5.1. The identity of the beneficiary has been verified in accordance with the provisions of customer due diligence as set out in the applicable legislation on AML/CFT and the information obtained on the basis of that verification has been stored in accordance with the provisions of Article 64 of the Law on AML/CFT and the Law on amending/supplementing the Law No. 05/L-096 on AML/CFT;
   5.2. The provisions of paragraph 1.4 of Article 19 of the Law on AML/CFT and the Law on amending and supplementing the Law No. 05/L-096 on AML/CFT apply to beneficiaries.

Article 17

Crypto-asset transfers with missing information on the initiator or beneficiary

1. The beneficiary crypto-asset service provider must implement effective risk-based procedures, including the risk-based procedures set out in the provisions of the applicable AML/CFT legislation on customer due diligence measures, to determine whether to execute, reject, return or suspend a crypto-asset transfer that does not contain complete required information on the initiator and beneficiary and to take appropriate follow-up actions.
2. Where the crypto-asset service provider of the beneficiary becomes aware that the information referred to in paragraphs 1 and 2 of Article 14 of this Regulation, or in Article 15 of this Regulation, is missing or incomplete, that crypto-asset service provider shall, on a risk-sensitive basis and without undue delay:
   2.1. refuse the transfer or return the transferred crypto-assets to the initiator's crypto-asset account; or
   2.2. request the required information on the initiator and beneficiary before crypto-assets are made available to the beneficiary.
3. Where a crypto-asset service provider repeatedly fails to provide the required information about the originator or beneficiary, the beneficiary's crypto-asset service provider must:
   3.1. take steps, which may initially include issuing warnings and setting time limits, before proceeding with refusal, restriction or termination in accordance with subparagraph 3.2 of this Article if the requested information has not yet been provided; or
   3.2. directly refuse any future transfers of crypto-assets from that crypto-asset service provider or restrict or terminate its business relationship with that crypto-asset service provider.
4. Based on the previous paragraph, the beneficiary's crypto-asset service provider must report this failure, and the steps taken, to the CBK and the FIU-K.

Article 18
Valuation and Reporting by the beneficiary's crypto-asset service provider

The beneficiary crypto-asset service provider should consider missing or incomplete information on the initiator or beneficiary as a factor when assessing whether a crypto-asset transfer, or any related transaction, is suspicious and whether it should be reported to the FIU in accordance with applicable AML/CFT legislation.

Subchapter III
Obligations for crypto-asset intermediary service providers

Article 19

Storage of information on the initiator and beneficiary accompanying the transfer

Crypto-asset intermediary service providers must ensure that all information received on the initiator and beneficiary accompanying a crypto-asset transfer is transmitted together with the transfer and that records of this information are retained and made available upon request to competent authorities.

Article 20
Disclosure of missing information on the initiator or beneficiary

The intermediary crypto-asset service provider shall implement effective procedures, including, where appropriate, monitoring after or during transfers, in order to detect whether the information on the initiator or beneficiary specified in subparagraphs 1.1, 1.2 and 1.3 of Article 14 of this Regulation and in subparagraphs 2.1, 2.2 and 2.3 of Article 14 of this Regulation has been submitted prior to, simultaneously with or in parallel with the transfer or batch transfer through the crypto-asset file, including in cases where the transfer is made from or to a self-hosted address.

Article 21

Crypto-asset transfers with missing information on the initiator or beneficiary

1. The intermediary crypto-asset service provider must implement effective risk-based procedures, including the risk-based procedures set out in the provisions of the applicable AML/CFT legislation on customer due diligence measures, to determine whether to execute, reject, return or suspend a crypto-asset transfer that does not contain complete required information on the initiator and beneficiary and to take appropriate follow-up actions.
2. Where an intermediary crypto-asset service provider becomes aware that the information referred to in paragraphs 1.1, 1.2 and 1.3 of Article 14 of this Regulation, and subparagraphs 2.1, 2.2 and 2.3 of Article 14 of this Regulation, or paragraph 1 of Article 15 of this Regulation is missing or incomplete, that intermediary crypto-asset service provider shall, on a risk-sensitive basis and without undue delay, :
   2.1. refuse the transfer or return the crypto-assets; or
   2.2. to request the required information on the initiator and beneficiary before carrying out the transfer of crypto-assets.
3. Where a crypto-asset service provider repeatedly fails to provide the required information about the originator or beneficiary, the intermediary crypto-asset service provider of the beneficiary must:
   3.1. take steps, which may initially include issuing warnings and setting time limits, before proceeding with refusal, restriction or termination in accordance with subparagraph 3.2 of this Article if the requested information has not yet been provided; or
   3.2. directly refuse any future transfers of crypto-assets from that crypto-asset service provider or restrict or terminate its business relationship with that crypto-asset service provider.
4. Based on the previous paragraph, the beneficiary's crypto-asset service provider must report this failure, and the steps taken, to the CBK and the FIU-K.

Article 22
Valuation and Reporting for Crypto-Asset Brokerage Service Providers

The crypto-asset intermediary service provider should consider missing or incomplete information on the initiator or beneficiary as a factor when assessing whether a crypto-asset transfer, or any related

transaction, is suspicious and whether it should be reported to the FIU in accordance with applicable AML/CFT legislation.

CHAPTER IV

COMMON MEASURES APPLICABLE TO PAYMENT SERVICE PROVIDERS AND CRYPTO-ASSET SERVICE PROVIDERS

Article 23
Policies, procedures and internal controls to ensure the implementation of preventive measures

Payment service providers and crypto-asset service providers must have policies, procedures and internal controls to ensure the implementation of AML/CFT measures under applicable legislation or the CBK Regulation on AML/CFT when carrying out transfers of funds and crypto-assets under this Regulation.

CHAPTER V

INFORMATION, DATA PROTECTION AND DATA RETENTION

Article 24
Data protection

1. The processing of personal data under this regulation is subject to the provisions of the Law on Personal Data Protection.
2. Personal data shall be processed by payment service providers and crypto-asset service providers under this Regulation solely for the purposes of preventing money laundering and terrorist financing and shall not be further processed in a manner incompatible with these purposes. The processing of personal data under this Regulation for commercial purposes is strictly prohibited.
3. Payment service providers and crypto-asset service providers shall provide new customers with the information required in accordance with the provisions of the Personal Data Protection Act before establishing a business relationship or carrying out an occasional transaction. This information shall be provided in a concise, transparent, intelligible and easily accessible form in accordance with the provisions of the Personal Data Protection Act and, in particular, shall include a general notice regarding the legal obligations of the payment service provider under this Regulation when processing personal data for the purposes of preventing money laundering and terrorist financing.
4. Payment service providers and crypto-asset service providers must always ensure that the transmission of any personal data to parties involved in the transfer of funds is carried out in accordance with the provisions of the Law on the Protection of Personal Data.

Article 25
Data storage

1. Information on the payer and the payee or on the initiator and the payee shall not be kept for longer than is strictly necessary. Payment service providers of the payer and the payee shall retain the information referred to in Articles 4 to 7 of this Regulation, and crypto-asset service providers of the initiator and the payee shall retain the information referred to in Articles 14 to 16 of this Regulation, for a period of five years.
2. Without prejudice to the following paragraph, after the expiry of the retention period referred to in paragraph 1 of this Article, payment service providers and crypto-asset service providers shall ensure that personal data are deleted, unless otherwise provided for by law.
3. The CBK may permit or require further retention for a maximum period of five years after having conducted a full assessment of the necessity and proportionality of such further retention, and where it considers it necessary for the prevention, detection or investigation of money laundering or terrorist financing.

Article 26
Cooperation with other authorities

The exchange of information between the CBK and other domestic and foreign authorities with competences in preventing and combating money laundering and terrorist financing will be subject to the provisions of the applicable AML/CFT legislation.

CHAPTER VI

ADMINISTRATIVE PENALTIES AND REMEDIAL MEASURES

Article 27
Administrative penalties and measures

1. Violations of the provisions of this regulation will be subject to corrective and punitive measures as defined by the Law.No.05/L-096 on AML/CFT and Law No. 08/L-333 on amending/supplementing the Law No. 05/L-096 on AML/CFT, the Law on the Central Bank and the relevant legislation on financial institutions.
2. The CBK will supervise financial institutions in terms of compliance with obligations under the applicable AML/CFT legislation, the AML/CFT Regulation and this Regulation.
3. The competent authorities (CBK and FIU-K) may coordinate their actions to impose administrative measures and sanctions, in accordance with the legislation in force, in any of the following ways:

   3.1. directly;

   3.2. in cooperation with each other.

Article 28
Specific provisions

1. The administrative penalties and measures set out in the provisions of Law No. 05/L-096 on AML/CFT and Law No. 08/L-333 on amending/supplementing the Law No. 05/L-096 on AML/CFT applies in case of the following violations of this regulation:

   1.1. repeated or systematic failure by a payment service provider to accompany the transfer of funds with the required information on the payer or the payee, in breach of Article 4, 5 or 6 of this Regulation, or by a crypto-asset service provider to accompany the transfer of crypto-assets with the required information on the initiator and the payee, in breach of Article 14 or 15 of this Regulation;

   1.2. repeated, systematic or serious failure by a payment service provider or crypto-asset service provider to maintain records, in breach of Article 25 of this Regulation;

   1.3. failure by a payment service provider to implement effective risk-based procedures, in breach of Article 8 or 12 of this Regulation, or by a crypto-asset service provider to implement effective risk-based procedures, in breach of Article 17 of this Regulation;

   1.4. serious failure by an intermediary payment service provider to comply with the requirements of Article 11 or 12 of this Regulation or by an intermediary crypto-asset service provider to comply with the requirements of Article 19, 20 or 21 of this Regulation.

Article 29
Reporting violations

1. The CBK, through its mechanisms, provides secure channels with the aim of encouraging reporting regarding violations of this regulation, these mechanisms include at least:

   1.1. specific procedures for receiving reports on violations and following them up;

   1.2. appropriate protection for employees of payment service providers and crypto-asset service providers who report violations committed within their institution;

   1.3. protection of personal data relating to both the person reporting the violations and the natural person suspected of being responsible for a violation, in accordance with the principles set out in the Law on the Protection of Personal Data;

   1.4. clear rules ensuring that confidentiality is guaranteed in all cases in relation to the person reporting violations committed within the obliged entity, unless disclosure is required by national law in the context of further investigations or subsequent judicial proceedings.

2. Payment service providers and crypto-asset service providers, in cooperation with competent authorities, should establish appropriate internal procedures for their employees to report breaches internally through a secure, independent, specific and anonymous channel, proportionate to the nature and size of the payment service provider or crypto-asset service provider.

CHAPTER VII

FINAL PROVISIONS

Article 30
Applicability

The provisions of this regulation, which determine the obligations of crypto-asset service providers, shall be implemented in accordance with the provisions of the Regulation on the Licensing of Crypto-Asset Service Providers.

Article 31
Repeal

With the entry into force of this regulation, the Regulation on information that must accompany transfers of funds, approved by the Board of the Central Bank on June 26, 2024, is repealed.

Article 32
Entry into force

This Regulation enters into force 10 (ten) days after the entry into force of the Law No. 08/L-328 on Payment Services, Law No. 08/L-333 on Amending and Supplementing the Law No. 05/L-096 on the Prevention of Money Laundering and Combating the Financing of Terrorism and Law No. 08/L-304 on Banks.

Dr. Sc. Bashkim Nurboja
Chairman of the Board of the Central Bank of the Republic of Kosovo