OVERVIEW

No. RADAR
6245

Responsible level
EU

Competent authority
EBA – European Banking Authority

Standard designation
Final Report on guidelines amending Guidelines EBA/GL/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849

Title of Standard
Final Report on guidelines amending Guidelines EBA/GL/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849

Abbreviation (standard)

Short Title

Abbreviation (standard)
EBA/GL/2024/01

Abbreviation
EBA/GL/2024/01

Implementation status of the standard
in draft / in consultation

Industry relevance
Banking, insurance

category
08. Anti-money laundering and financial sanctions

Document type

Guideline

Management Summary

These guidelines supplement the guidelines set out in Articles 17 and 18(4) of the*Directive (EU) 2015/849 on due diligence measures and the factors that credit and financial institutions should take into account when assessing the risk of money laundering and terrorist financing associated with individual business relationships and occasional transactions (Dataset 4032)*changed.

The amendment specifically includes factors that crypto asset service providers (CASPs) should consider. Key points of the amendment include:

- highlighting specific risk factors that reflect the particular characteristics of crypto-assets and CASPs and that should be considered by credit and financial institutions when entering into a business or correspondent relationship with CASPs;

- the establishment of secure tools for remote onboarding at credit and financial institutions;

- new sector-specific guidelines for CASPs in Title II, explaining the risk-enhancing and risk-mitigating factors that CASPs should consider when assessing the risks associated with their client business relationships;

- Guidance on mitigating measures that CASPs should apply in situations where the risk is either increased or reduced.

Management Summary

The present guidelines amend the*Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (dataset 4032)*.

The amendment specifically includes factors that crypto-asset service providers (CASPs) should consider. Key points of the amendment include:

- highlighting specific risk factors that reflect the unique characteristics of crypto-assets and CASPs and that should be considered by credit and financial institutions when entering into a business or correspondent relationship with CASPs;

- the establishment of secure remote onboarding tools for credit and financial institutions;

- new sector-specific guidance for CASPs in Title II explaining the risk-increasing and risk-mitigating factors that CASPs should consider when assessing the risks associated with their customer business relationships;

- guidance on risk mitigation measures that CASPs should apply in situations where risk is either increased or decreased.

CONTENTS

Main content

B. Essential content

These guidelines amend the guidelines set out in Article 17 and Article 18(4) of the *Directive (EU) 2015/849 on due diligence measures and the factors that credit and financial institutions should take into account when assessing the risk of money laundering and terrorist financing associated with individual business relationships and occasional transactions (Dataset 4032)*. The content refers to this guideline unless otherwise stated. Changes to the guidelines are described in Section 3 of this document.

I. Changes to the subject matter, scope and definitions Paragraph 12 adds that in addition to the definitions of this guideline, the definitions of *Directive (EU) 2015/849 (4th Anti-Money Laundering Directive, Dataset 849)* and now also the definitions of *Regulation (EU) 2023/1113 of the European Parliament and of the Council on information accompanying transfers of funds and transfers of certain crypto-assets and amending Directive (EU) 2015/849 (Dataset 4970)* are relevant for the definition of this guideline.

II. Amendments to Guideline 1: Risk assessments: Main principles for all companies Keep risk assessment up to date
The obligation under Guideline 1.7 to maintain systems and controls to keep individual and enterprise-wide risk assessments for money laundering and terrorism (ML/TF) risks up to date is extended to new products, new services, business practices, new delivery channels, or new technologies that are part of the ML/TF systems and control framework. ML/TF risks should be assessed prior to the implementation of the new products or technologies and considered in the enterprise-wide risk assessment, policies, and procedures in accordance with Article 8(2) of Directive (EU) 2015/849.

III. Amendments to Guideline 2: Determination of ML/TF risk factors Risk factors related to customers
Guideline 2.4 b) adds services related to crypto-assets within the meaning of Guidelines 9.20 and 9.21 as a new risk sector with increased ML/TF risk.

IV. Amendments to Guideline 4: Customer due diligence obligations to be applied by all undertakings

1. Situations without personal contact

Guideline 4.29 adds that in order to fulfil the general due diligence obligations when initiating business relationships or processing transactions without personal customer contact, the *Guidelines on the use of applications for the remote customer acceptance process pursuant to Article 13(1) of Directive (EU) 2015/849 (EBA/GL/2022/15) (Dataset 5191)* must be observed.

2. Use of innovative technological means to verify identity

If technologies from an external provider based in a non-EU country are used to establish and verify a customer's identity, in addition to the other requirements of Guideline 4.35 (understanding the associated legal risks, operational risks and data protection requirements), it must be ensured that the outsourcing company has immediate access to the relevant customer data and information, even in the event of termination of an outsourcing agreement (see source for details).

3. Unusual transactions

a) Guideline 4.60 adds an example of unusual transactions for which appropriate policies and procedures must be established. This defines transactions that deviate from the usual frequency, including transactions involving small amounts or consecutive transactions without a coherent economic rationale, as "unusual transactions."

b) The measures to identify suspicious transactions under Guideline 4.61 a) must now also include the origin and destination of crypto-assets.

4. Transaction monitoring

Guideline 4.74 b) adds that the use of automated systems for transaction monitoring should be considered not only for high transaction volumes, but also for high-frequency trading. Furthermore, the new Guideline 4.74 d) adds the use of sophisticated analytical tools, such as distributed ledger analysis tools, as an additional possible instrument for transaction monitoring.

V. Amendments to Guideline 6: Training

Guideline 6.2 c) clarifies that employees' understanding of suspicious or unusual transactions should develop, particularly with regard to the nature of the products and services offered by the company. According to the new Guideline 6.2 d), employees should also understand the use of automated systems for monitoring transactions and business relationships, including sophisticated analytical tools, as well as the interpretation of the results of these systems and tools.

VI. Amendments to Guideline 8: Sector-specific guideline on correspondent banking relationships

1. Risk factors related to customers

a) In Guideline 8.6 d), the examples of respondent bank transactions in sectors with increased ML/TF risk are supplemented by two further examples. Newly included are transactions in their own name or on behalf of, or direct transactions with, crypto-asset service providers (CASPs) established in a third country that do not meet the requirements of *Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets and amending Regulation (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA, Dataset 4445)* or equivalent requirements such as the 4th Anti-Money Laundering Directive. Businesses that are carried out in the company’s own

executed on behalf of or on behalf of CASP and enable transfer to and from self-managed server addresses.

b) According to the new Guideline 8.6 h), the establishment of IBAN customer accounts with respondent CASPs for the receipt of funds in an official currency poses an increased ML/TF risk if the respondent CASP does not hold those accounts or is not known to be linked to the respondent CASP.

2. Risk factors related to countries or geographical areas

According to the new Guideline 8.8 d), an increased ML/TF country risk exists if the respondent institution cannot determine with sufficient certainty whether a customer is domiciled in a high-risk country within the meaning of Guideline 8.8 a) in conjunction with Article 9 (2) of the 4th Anti-Money Laundering Directive or a country with corruption. An increased risk is also assumed if the respondent institution cannot determine the IP address of its customers if its internal policies and procedures require this.

3. Respondent institutions based outside the EEA

Guideline 8.17 a) extends the requirement to collect sufficient information about the respondent institution to respondent CASPs. When assessing the risk of the respondent CASP, the type of crypto assets transferred via the correspondent account must also be considered. According to the addition in Guideline 8.17 c), when assessing the respondent institution's control mechanisms, the transaction monitoring tools it uses must also be considered.

VII. Amendments to Guideline 9: Sector-specific guideline on standardised retail banking

Guideline 9.3 adds that banks offering asset management services must also comply with sector-specific Guideline 12 and CASP must comply with the new sector-specific Guideline 21.

1. Collective accounts

According to the addition to Guideline 9.16, general customer due diligence obligations must also be observed for omnibus accounts for crypto assets. The addition to Guideline 9.17 clarifies that the basis for determining a high ML/TF risk is the ML/TF risk assessment conducted in accordance with this Guideline. Guideline 9.18 adds that the application of simplified due diligence obligations also depends on the customer's individual ML/TF risk assessment.

2. Customers offering services related to crypto assets

a) The heading has been reworded. Guidelines 9.20 to 9.23 on virtual currency services are replaced by new Guidelines 9.20 and 9.21, which contain rules for commencing business with unregulated CASPs.

b) The minimum due diligence obligations defined in Guideline 9.21 correspond to the obligations of the previous Guideline 9.23 a) to d) (including dialogue with customers, extension of due diligence obligations to the customer's senior management level). According to Guideline 9.21 e) and the new Guideline 9.21 f), it must be determined whether the services offered by the customer are covered by the customer's registration or license and/or whether the customer also provides other regulated or authorised services as a credit or financial services institution. According to the new Guideline 9.23 g), it must also be determined whether the issuance of crypto assets to raise funds, including through Initial Coin Offerings (ICOs), is legally permissible, regulated with regard to ML/TF, and complies with international standards, such as those published by the FATF.

VIII. Amendments to Guideline 10: Sector-specific guideline for e-money issuers, Amendments to Guideline 15: Sector-specific guideline for investment firms

For e-money issuers and investment firms, Guideline 10.2 (e-money issuers) and Guideline 15.1 (investment firms) add that they must also comply with the new sector-specific Guideline 21 if they also act as CASPs.

IX. Amendments to Guideline 17: Sector-specific guideline for regulated crowdfunding platforms

Guideline 17.4 i) specifies that an increased ML/TF risk factor exists for products, services, and transactions if the crowdfunding service provider allows payments in crypto assets via the crowdfunding platform. An increased customer risk also exists according to Guideline 17.6 b) if the investor or project promoter forwards crypto assets.

X. Guideline 21: Sector-specific guideline for crypto service providers (CASPs)

The new Guideline 21 regulates the sector-specific requirements for CASPs. In this sector, ML/TF risks arise primarily from the specific business model and technology used, which enables the global transfer of crypto assets and the servicing of customers in different jurisdictions. Like the other guidelines in Title II, Guideline 21 must be considered in conjunction with the requirements of Title I and Guideline 8. The due diligence requirements largely correspond to the due diligence requirements for other sectors, but have been adapted to the specific characteristics of CASPs.

1. Risk factors related to products, services and transactions

a) Products or services offered by CASPs offer a high degree of anonymity.

Other factors that trigger an increased risk, according to Guideline 21.3 b) and c), include payment by third parties who are neither connected with the product nor previously identified, as well as a lack of restrictions on the volume or maximum values of transactions.
Guideline 21.3 d) lists, among other things, technology-related risk factors such as self-managed addresses, peer-to-peer cryptocurrency exchange platforms or mixer or tumbler platform management, management of crypto asset accounts or distributed ledger addresses by CASPs that are not subject to EU regulation or comparable regulations, the decentralised or distributed use of crypto assets that is not controlled by a legal or natural person (often referred to as decentralised finance, decentralised finance, DeFi), crypto automated teller machines (crypto ATMs) or other hardware that provides for the use of cash or electronic money and benefits from the exemptions for e-money under Article 12 of the 4th Anti-Money Laundering Directive.

According to Guideline 21.3 e), further risks arise from new business practices, including new delivery channels and the use of new technologies whose ML/TF risks are not yet fully understood. Furthermore, an increased risk is to be assumed if, according to Guideline 21.3 f), so-called nested services (a service within a service) are offered by wholesale CASPs for which the wholesale CASP exercises only weak controls over this service, and if, according to Guideline 21.3 g), the results of an analysis using an analysis tool indicate an increased level of risk (see source for details).

b) Risk-reducing, on the other hand, is defined in Guideline 21.4 a) as products with reduced functionality, such as low transaction volumes, and in accordance with Guideline 21.4 b) as transactions on crypto-asset accounts or distributed ledger addresses in the name of customers held by a CASP established in a third country where the regulatory requirements are equivalent to those of the MiCA Regulation and amending Directive (EU) 2019/1937 or the 4th Anti-

Comply with the Money Laundering Directive. The same applies to transactions on bank accounts at a credit institution. Depending on the type and purpose of the payment channel or system, closed-loop systems or systems that allow micropayments or government-to-person payments (or vice versa) are classified as risk-reducing according to Guideline 21.4 c) and d). Products that are only available to certain customer categories, e.g., employees of the company issuing the crypto asset, are also considered risk-reducing.

2. Risk factors related to customers

a) Guideline 21.5 a) and b) lists a number of risk factors that are considered to increase risk and relate to the type of customer and their behavior. Depending on the type of customer, factors considered to increase risk within the meaning of Guideline 21.5 a) include, among others, non-profit organizations that demonstrably sympathize with extremism and/or terrorism, shell companies, companies or individuals that use IP addresses on the dark web, and individuals with limited knowledge of the crypto-asset business (see source for details).

b) According to Guideline 21.5 b), risk-increasing factors based on the customer's behavior include, among others, the opening of multiple crypto-asset accounts with the CASP, the lack of identification documents of the beneficial owner without justifiable reason, the use of an IP address used by multiple customers, the frequent changing of personal information or means of payment, the persistent circumvention of due diligence requirements if the transactions are always just below the relevant threshold, and certain behaviors when exchanging crypto-assets for official currencies or vice versa (see source for details).

c) Risk-reducing factors include, among others, compliance with the requirements for the exchange of customer data between financial intermediaries (travel rule) according to the new version of the Regulation on the transmission of information accompanying transfers of funds and the information requirements set out in Regulation (EU) 2023/1113 for previous crypto-asset transactions, the customer being known from previous business relationships and/or the origin or destination for a currency exchange being a customer bank account with a credit institution located in a country whose risk has been assessed as low by the CASP (see source for details).

3. Risk factors related to countries or geographical areas

a) The country risks in Guideline 21.7 a) and b) correspond to the country risks in Guideline 9.8 a) and b) to standardized retail banking. Further country risks include the customer's or their beneficial owner's domicile in a high-risk ML/TF country (Guideline 21.7 c)), the establishment of a business relationship via a CASP or crypto ATMS domiciled in a high-risk non-EU country (Guideline 21.7 d)), and, in accordance with Guideline 21.7 e), customer involvement in the mining of crypto assets (either directly or indirectly through relationships with third parties) carried out in high-risk countries.

b) The risk-mitigating factors under Guideline 21.8 a) are essentially the same as Guideline 9.9, but have been adapted to crypto-asset services (see source for details).

4. Risk factors related to distribution channels

a) An increased risk is to be assumed if the business relationship according to Guideline 21.9 was established via identification applications that do not comply with the guidelines on the use of applications for the remote customer acceptance process according to Article 13 (1) of Directive (EU) 2015/849 (EBA/GL/2022/15), there are no restrictions on the type of financing instrument (e.g. in the case of cash, cheques, e-money products that fall under the exemption of Article 12 of the 4th Anti-Money Laundering Directive), the business relationship was established via an intermediary in the crypto-

asset sector based outside the EU that is unregulated or not subject to equivalent ML/TF requirements within the meaning of the 4th Anti-Money Laundering Directive, new technologies or distribution channels are used, or the business relationship was established via a crypto ATM.

b) Risk is mitigated, however, if the CASP can rely on the customer due diligence measures of a third party established in the EU in accordance with Article 26 of the 4th Anti-Money Laundering Directive.

5. Measures

The requirements for systems for identifying ML/TF risks as defined in Guideline 21.11 correspond to the requirements of Guideline 9.12. Therefore, CASPs must also comply with the requirements of Title I. Furthermore, CASPs should ensure that they have adequate transaction monitoring, employ sophisticated analytical tools, and provide dedicated training to relevant staff (see source for details).

6. Increased customer due diligence

a) According to Guideline 21.12, CASPs must comply with enhanced due diligence obligations pursuant to Article 18(4) of the Anti-Money Laundering Directive if a business relationship or occasional transaction presents an increased risk. The enhanced due diligence obligations essentially correspond to Guidelines 21.12(a) to (c) and are adapted to the specific characteristics of crypto-asset services. The examples of additional customer information to be collected in Guideline 21.12(c) are expanded. For example, in addition to the origin of the crypto-assets or the customer's official currency, information can be obtained about the time and place of acquisition of the assets and the customer's trading history (see source for details).

b) Information on the origin of crypto assets must be obtained for all transactions with increased risk, in accordance with Guideline 21.12 d).

c) Guideline 21.12 e) to m) provide further examples and measures for enhanced due diligence. For example, for customers with addresses in multiple distributed ledger or blockchain networks, the CASP should link all addresses to the same customer. Furthermore, the frequency of IP address monitoring can be increased and a customer's IP address can be compared with those used by other customers (see source for details).

d) According to Guideline 21.13, CASPs should use advanced analysis tools in addition to standard analysis tools, particularly for transactions with self-managed server addresses. These tools are essential for tracing transactions and identifying criminal activities, individuals, or organizations. For business relationships or transactions with high-risk third countries, CASPs must comply with Guideline 21.14, Title I.

7. Simplified customer due diligence obligations

If a situation has been classified as low risk based on the CASP's risk analysis and this is permitted under national law, simplified due diligence measures may be applied in accordance with Guideline 21.15. For CASP, according to Guideline 21.15 a) and b), this concerns the identification of clients subject to legal authorisation and regulatory requirements in the EU or a non-EU country and the updating of information when certain triggering events occur. Furthermore, according to Guideline 21.15 c), the frequency of transaction monitoring may be reduced for recurring transactions, e.g., in portfolio management.

8. Records

According to Guideline 21.16, CASPs may not rely on customer information in the distributed ledger to fulfill their record-keeping obligations. Instead, the record-keeping obligations under the 4th Anti-Money Laundering Directive and Sections 5.1 and 5.2 of these Guidelines must be observed. CASPs should implement procedures to assign distributed letter addresses to a private key (see source for details).

CATEGORIZATION

Keywords

Airdrop, general due diligence, crypto service provider, record, automated system, bank account, cash, blockchain network, CASP, closed-loop system, Crypto Automated Teller Machines, decentralized finance, DeFi, distributed ledger, e-money issuer, increased ML/TF risk, EU country, official currency, advanced analysis tool, money laundering and terrorism risk, non-profit organizations, business relationship, business relationship without personal contact, governance token, government-to-person, wholesale CASP, ML/TF risk, high-risk country, ICO, initial coin offering, innovative technology, Internet protocol, IP anonymizer, IP address, crypto lending protocol, crypto asset, crypto ATM, customer, customer due diligence, country risk, shell company, micro-payment, mining, nested service, non-EU country, portfolio management, respondent CASP, respondent institution, ring signatures, risk assessment, risk sector, collective account, crowdfunding service,
Crowdfunding platform, self-managed server address, staking reward, standardized retail banking, stealth address, transaction monitoring, unusual transaction, unregulated CASP, suspicious transaction, simplified due diligence, asset management, obfuscated ledger technology, enhanced due diligence, hidden service, virtual currency, currency exchange, investment firm

Legal and information bases

- Guidelines on the use of applications for the remote customer acceptance process pursuant to Article 13(1) of Directive (EU) 2015/849 (EBA/GL/2022/15) (Dataset 5191)
- Regulation (EU) 2023/1113 (recast FTR, dataset 4970)
- Regulation (EU) 2023/1114 (MiCA, dataset 4445)
- Guidelines pursuant to Article 17 and Article 18(4) of Directive (EU) 2015/849 on due diligence measures and the factors that credit and financial institutions should consider when assessing the risk of money laundering and terrorist financing associated with individual business relationships and occasional transactions (Dataset 4032)
- Directive (EU) 2015/849 (4th Anti-Money Laundering Directive, Dataset 897)
- Regulation on information accompanying transfers of funds and repealing Regulation (EU) No 1781/2006 (FTR, dataset 896)

Related Standards

- Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (dataset 4032)

Target group – credit institutions
Yes

Target group – financial services institutions
Yes

Target group – Other companies in the financial sector
Yes

Target group – payment institutions
Yes

Target group – insurance companies
Yes

Target group – supplement
These guidelines are addressed to credit and financial institutions within the meaning of Article 3(1) and (2) of Directive (EU) 2015/8497 and to competent authorities within the meaning of Article 4(2)(iii) of Regulation (EU) 1093/2010.

Comments
These are addressed to credit and financial institutions as defined in Article 3(1) and 3(2) of Directive (EU) 2015/8497 and to competent authorities as defined in Article 4(2) point (iii) of Regulation (EU) 1093/2010.

Statement by (date)

Implementation status Explanation
Final report

Status – Further Details
Final report

Date of entry into force/publication
December 30, 2024

Entry into force estimated?
No

Date of first application
December 30, 2024

Application appreciated?
No

Date Standard repealed

Remark (Entry into force/Publication)

The competent authorities must notify, in all official EU languages, within two months of the publication of the guidelines, whether they comply or intend to comply with the guidelines or give reasons why they do not comply or intend not to comply (comply-or-explain).

The guidelines are to be applied from 30 December 2024.

Comments

Competent authorities must notify the EBA within two months after the publication of the translations as to whether they comply or intend to comply with these guidelines, or otherwise state their reasons for noncompliance (comply-or-explain).

These guidelines will apply from December 30, 2024.

Sources

The sources are not shown in this working paper.