OPEN DIALOGUE

IMPACT OF THE EU AND FATF REGULATORY FRAMEWORKS ON NON-CUSTODIAL CRYPTO-ASSETS WALLETS

22 DECEMBER 2024

The Open Dialogue Foundation (ODF) was established in Poland in 2009 on the initiative of Ukrainian student and civic activist Lyudmyla Kozlovska (who currently serves as President of the Foundation). Since its founding, statutory objectives of the Foundation include the protection of human rights, democracy and the rule of law in the post-Soviet area. In July 2017 the area of interest of the Foundation was expanded due to the rapidly deteriorating situation in Poland and other EU member states affected by illiberal policies implemented by their populist governments. The Foundation has its permanent representations in Brussels, Warsaw and Kyiv.

This Report has been prepared by Gracjan Pietras, advocate and Marcin Liszka, attorney-at-law on the request of the Open Dialogue Foundation on behalf of the Building True Change Coalition (BTC Coalition). The Testimonials included within it are attributed to the individuals as described therein. The Building True Change Coalition (BTC Coalition) composed of human rights defenders, political activists, Bitcoin entrepreneurs, and industry experts and coordinated by the Open Dialogue Foundation. The BTC Coalition aims to: (1) combat the abuse of Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) within the wider range of transnational repression mechanisms; (2) promote financial inclusion in non-democratic and developing countries; (3) promote Bitcoin and stablecoins as tools to support human rights efforts and provide humanitarian aid worldwide; and (4) educate on the role of Bitcoin mining as an instrument to facilitate the adoption of renewable energy sources.[1]

Website: https://odfoundation.eu/

e-mail: odfoundation@odfoundation.eu

X: @ODFoundation

Authors:

Gracjan Pietras, Advocate & Partner at DJP (djp.pl), Columnist at iMagazine.pl. With over 25 years of experience in the field of intellectual property and new technologies, Gracjan Pietras is widely recognized on the Polish market. He provides legal advice to notable companies from various market sectors on the acquisition of advanced IT systems and related services. He has been listed as a recommended lawyer in The Legal 500 EMEA editions of 2019-2024 for TMT (Technology, Media, and Telecommunications) and Dispute Resolution. Email: gpietras@djp.pl

Marcin Liszka, legal advisor, senior associate at DJP (djp.pl), has 7 years of experience in the field of intellectual property and new technologies. He has participated in numerous transactions related to the acquisition and maintenance of IT solutions involving the transfer, licensing, and provision of IT and media products. He has also advised businesses involved in Bitcoin-related activities to help them comply with MiCA regulations, AML (Anti-Money Laundering) requirements, and other relevant regulations. He has been recognized as a recommended lawyer in The Legal 500 EMEA 2023 and 2024 edition for TMT (Technology, Media, and Telecommunications). Email: mliszka@djp.pl

Project Manager: Lyudmyla Kozlovska (the Open Dialogue Foundation): lyudmylakozlovska@odfoundation.eu

Disclaimer

The information herein reflects the authors' expertise and the most reliable data available at the time of writing. However, this report does not constitute legal advice, and neither the authors nor the Open Dialogue Foundation shall be liable for any actions taken based on its content.

Objective

This report provides an analysis of the current and forthcoming regulatory frameworks within the European Union laws, based on the FATF's recommendations, concerning non-custodial Bitcoin and other crypto-assets wallets ("**non-custodial wallets**") and peer-to-peer cryptocurrency transactions ("**P2P transactions**"). The primary aim is to determine whether, and to what extent, non-custodial wallets fall within the purview of public regulatory systems. Additionally, it evaluates the potential implications of such frameworks for entities and individuals engaging in non-custodial wallet activities, particularly regarding Anti-Money Laundering ("**AML**") and Counter-Terrorist Financing ("**CFT**") requirements.

The European Union plays a central role in shaping global financial regulatory standards. However, the current restrictive approach towards privacy-enhancing payment tools, such as self-hosted wallets and mixers, presents significant challenges. These restrictions limit financial freedoms for individuals and entities within the EU and third countries, particularly those already marginalised or financially excluded. Furthermore, such measures may unintentionally enable illiberal regimes to exert financial repression by restricting access to secure and private financial tools.

In preparing this report, the authors have considered the ongoing discussions on the EU's global competitiveness and the critical need for effective financial instruments to support civil society organisations addressing human rights violations and humanitarian crises in third countries. Particular attention has been given to the calls from the Open Dialogue Foundation, representing the Building True Change Coalition, for a reassessment of the EU's regulatory stance. They advocate for the removal of restrictive provisions targeting privacy-enhancing payment tools to ensure that EU regulations uphold fundamental rights, facilitate humanitarian efforts, and strengthen the Union's position as a global leader in promoting democratic values.

Table of Contents:

1. EXECUTIVE SUMMARY

- The current regulatory landscape for non-custodial wallets and P2P transactions is evolving, particularly in light of the European Banking Authority ("**EBA**") revised guidelines and forthcoming regulations. As of the date of this report, the existing AML directive does not impose specific requirements on non-custodial wallets. However, the EBA's Guidelines EBA/2021/02 highlight the elevated risks associated with these wallets, particularly concerning customer due diligence for transactions involving non-custodial addresses and decentralised platforms. According to the guidelines, key risk factors include frequent transactions just below the €1,000 threshold, immediate withdrawals to non-custodial addresses, and the use of anonymity-enhancing tools.
- The forthcoming Markets in Crypto-Assets Regulation and Regulation (EU) 2023/1113 will come into effect on 30 December 2024. The former focuses on the regulatory obligations of crypto-asset service providers (CASPs) rather than AML/CFT issues. However, it may indirectly influence CASPs to adopt stricter practices regarding non-custodial wallets.
- Regulation (EU) 2023/1113 will directly influence CASPs in various ways as it requires CASPs to collect detailed information on transactions involving non-custodial wallets and report suspicious activities. In practice, CASPs will be prohibited from facilitating anonymous transactions. Also, the regulation imposes stringent obligations on CASPs concerning customer due diligence when engaging with non-custodial addresses. It should be noted that the fulfilment of these obligations will likely lead to an increase in operational costs for CASPs, necessitating the implementation of advanced analytics tools, the hiring of AML-qualified personnel, and other related expenditures. Consequently, to mitigate costs and reduce the risks associated with transfers to and from non-custodial addresses, CASPs may opt to decline such transfers altogether.
- The obligations imposed on CASPs conflict with the rise of open-source technologies like the Lightning Network, Fedimint, and e-cash, which are permissionless, censorship-resistant, and provide strong privacy guarantees. These rapidly growing technologies are reshaping global transaction patterns, and by rejecting such transactions, EU-based CASPs risk losing market share and being outcompeted by non-European rivals operating under less restrictive frameworks. This regulatory approach may marginalise EU CASPs, pushing users toward unregulated alternatives outside the EU, thereby undermining the effectiveness of the AML/CFT framework. The result is not only a failure to meet regulatory objectives but also a weakening of the EU's digital economy, innovation capacity, and global competitiveness in financial services.
- Looking ahead, the AML Regulation (EU) 2024/1624 and the AML Directive (EU) 2024/1640, set to take effect by July 10, 2027, will introduce even more stringent regulations for non-custodial wallets and P2P transactions. These regulations will impose enhanced customer due diligence obligations on CASPs, including risk assessments and monitoring of transactions involving non-custodial addresses. The FATF also emphasizes the need for a risk-based approach to address the unique challenges posed by non-custodial wallets and P2P transactions, urging member states to enhance transparency and oversight.
- In conclusion, while current regulations do not specifically target non-custodial wallets, upcoming legislation and guidelines will significantly impact how these wallets are managed

within the financial ecosystem, potentially leading to increased scrutiny and operational costs for CASPs.

- AML and CFT regulations requiring CASPs to collect and disclose extensive customer data, including information on non-custodial wallets and transactions, pose significant risks to financial privacy. While financial privacy is a fundamental right enshrined in international and EU legal frameworks, these regulations often lack harmonised procedural safeguards and rely on Member States for implementation. Criticisms include the absence of judicial oversight, excessive data sharing, and insufficient ties to criminal investigations, as highlighted by rulings of the Court of Justice of the European Union (CJEU). This regulatory framework risks violating privacy rights and enabling misuse of data for purposes beyond crime prevention, such as political objectives, underscoring the need for robust safeguards to balance privacy with crime prevention objectives.

2. CURRENT STATUS OF NON-CUSTODIAL WALLETS (UNTIL 30 DECEMBER 2024) IN THE EU

The current AML directive[1] does not provide for any specific requirements relating to non-custodial wallets. However, the EBA has issued revised guidelines on customer due diligence[2] ("**Guidelines EBA/2021/02**"), introducing potentially stringent obligations for obliged entities when engaging with customers who utilise non-custodial addresses. Guidelines EBA/2021/02 highlight that non-custodial wallets, as a technological solution, pose an elevated risk in terms of AML and CFT compliance.

The following scenarios have been, in particular, identified as contributing to an elevated AML/CFT risk:

1. Frequent receipt or transfer of crypto-assets from non-custodial addresses in amounts just below the €1,000 threshold.
2. Immediate withdrawal of crypto-assets from a CASP to a non-custodial address following their deposit or exchange within the CASP.
3. Utilisation of anonymity-enhancing tools, such as crypto-asset ATMs or protocols enabling cross-network exchanges (e.g., Monero, Zcash), which are indirectly associated with non-custodial wallets.
4. Repeated transactions involving crypto-assets sent to or received from:
   - Multiple non-custodial addresses or numerous crypto-asset accounts held by the same or different CASPs without any clear economic rationale.
   - Non-custodial addresses on decentralised platforms employing mixers, tumblers, or other privacy-enhancing technologies that obscure transaction histories linked to distributed ledger addresses.
   - Crypto-asset accounts frequently operating below a defined threshold or, in cases involving transfers to non-custodial addresses, below the €1,000 threshold.

[1] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

[2] Final Report of 16 January 2024 - Guidelines amending Guidelines EBA/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; (EBA/GL/2024/01).

In such cases, CASPs will be required to implement enhanced customer due diligence measures. These measures may include verifying the customer's identity, gathering additional information about the customer and the nature and purpose of the business relationship, and constructing a more comprehensive customer profile. This process could involve determining the source of the customer's wealth and funds, clarifying the purpose of specific transactions, and obtaining confirmation that a non-custodial address used for a transfer is controlled or owned by the CASP's customer. CASPs are also expected to employ advanced analytics tools to assess transaction risks, particularly for transactions involving non-custodial addresses. These tools enable CASPs to trace transaction histories and identify potential connections to criminal activities, individuals, or entities.

The key potential consequences of the EBA's Guidelines (EBA/2021/02) include the following:

1. A discouragement of customers from utilizing non-custodial wallets due to increased scrutiny and restrictions.
2. CASPs refusing to accept transactions originating from non-custodial addresses.
3. A potential violation of the right to financial privacy, as governments may gain access to data collected by CASPs.
4. Banks refusing to cooperate with CASPs that process transactions involving non-custodial wallets.
5. Acceptance of transactions from non-custodial wallets by CASPs potentially leading to a negative reassessment of the credit institution's exposure to operational risk, which may adversely impact the CASP's creditworthiness.

3. FORTHCOMING REGULATIONS

3.1. The Markets in Crypto-Assets Regulation 2023/1114 ("MiCA")[3]

MiCA is scheduled to enter into force on 30 December 2024. While it adopts a broad and comprehensive approach, MiCA explicitly excludes "*hardware or software providers of non-custodial wallets*" from its scope, ensuring that non-custodial wallets and peer-to-peer (P2P) transactions are not directly affected by its provisions.

MiCA primarily focuses on requirements for the public offering and admission to trading of crypto-assets, as well as regulatory obligations for CASPs, rather than addressing AML/CFT matters. However, MiCA may provide a basis for supervisory authorities to influence CASPs by defining standards for market practices and policies. This could indirectly lead to stricter requirements or more cautious practices concerning non-custodial wallets and P2P transactions imposed by CASPs as part of their compliance measures.

3.2. Regulation (EU) 2023/1113 on Information Accompanying Transfers of Funds and Certain Crypto-Assets[4]

The regulation will enter into force on 30 December 2024.

[3] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

[4] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

Transactions involving crypto-assets conducted solely between individuals without the involvement of a CASP are excluded from the scope of this regulation. As a result, any P2P transfers between two or more non-custodial wallet addresses will remain outside the regulatory framework.

Any transactions involving CASPs will fall into a strict regulatory framework. In particular:

1. CASPs will be required to collect information on both the originator and beneficiary of the transfer and to perform a risk assessment related to the transaction (Collection and Risk Assessment).
2. CASPs will be obliged to report any suspicious transactions, including those originating from non-custodial wallets, to the relevant AML/CFT authorities (Reporting Suspicious Transactions or RST).
3. CASPs will need to reject transactions or terminate cooperation (Rejection and Termination) in cases where (a) verification of the required data for transfers involving non-custodial wallets is not possible; and/or (b) there is suspicion that the transaction is being executed for illicit or prohibited purposes.

In the Travel Rule Guidelines of 4 July 2024[5], the EBA provides clarification regarding the expectations placed upon CASPs concerning the implementation of effective procedures for the detection and management of crypto-asset transfers. This includes transfers that involve non-custodial wallets. The EBA emphasises the necessity for CASPs to establish robust mechanisms that facilitate the identification and oversight of all crypto-asset transfers, ensuring compliance with regulatory requirements and the mitigation of associated risks. This guidance aims to enhance the operational integrity of CASPs in their dealings with both custodial and non-custodial wallet transactions.

The following key remarks pertain to the management of non-custodial wallets by CASPs:

1. In instances where a non-custodial address is utilised as the endpoint of a transfer, the CASP is required to collect pertinent information regarding the originator or beneficiary from their customer. Should the CASP fail to obtain the necessary information, it retains the right to reject, return, suspend, or execute the transfer in accordance with its risk-based policies. Furthermore, the CASP should evaluate the future handling of the non-custodial address, which may include rejecting any subsequent transfers to or from such an address or terminating its business relationship with it.
2. The CASP must ascertain whether a transfer involving a non-custodial address meets or exceeds the threshold of € 1,000 at the time the transfer is ordered or initiated, in the case of the originator's CASP, or at the time of receipt, in the case of the beneficiary's CASP.
3. The CASP is responsible for assessing whether the non-custodial address is owned or controlled by the originator or beneficiary. This assessment may be conducted using one or more of the following verification methods:
    - Unattended verifications as outlined in the Guidelines on the Use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849, which display the address.
    - Attended verification as specified in the same Guidelines.

[5] EBA Final Report on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 (Travel Rule Guidelines) dated 4 July 2024.

- The transfer of a predefined amount (preferably the smallest denomination of the relevant crypto-asset), as determined by the CASP, from and to the non-custodial address to the CASP's account.
- Requesting the customer to digitally sign a specific message within the account and wallet software using the key corresponding to that address.
- Other appropriate technical means that ensure a reliable and secure assessment, provided that the CASP is fully satisfied with its knowledge of the ownership or control of the address.

4. CASP will have to assess risk associated with transfers from or to a non-custodial address.

CASPs will, therefore, be expressly prohibited from facilitating anonymous transactions. The regulation, along with its accompanying guidelines, imposes a series of stringent obligations on CASPs concerning customer due diligence when engaging with non-custodial addresses.

Consequently, the fulfilment of these obligations may lead to an increase in operational costs for CASPs, necessitating the implementation of advanced analytics tools, the hiring of AML-qualified personnel, and other related expenditures. Consequently, there exists a potential risk that CASPs, in an effort to mitigate costs and reduce the risks associated with transfers to and from non-custodial addresses, may opt to decline such transfers altogether.

The obligations imposed on CASPs also conflict with the rapid development of emerging open-source technologies such as the Lightning Network, Fedimint, and e-cash. These technologies, characterised by their permissionless and censorship-resistant nature, provide users with strong privacy guarantees and are accessible to any interested party. Their share of global transactions has been increasing significantly and is expected to continue growing.

By restricting or rejecting transactions conducted using these technologies, CASPs operating within the EU risk marginalisation in the global market. Such regulatory limitations disadvantage CASPs by excluding them from a rapidly expanding sector, reducing their ability to compete effectively with non-European service providers who face fewer restrictions. This, in turn, could lead to a significant loss of business opportunities, innovation potential, and global market share for EU-based entities.

Furthermore, the regulatory framework may inadvertently encourage the circumvention of regulated CASPs by driving users towards unregulated or less-regulated entities outside the EU. This shift would undermine the effectiveness of the AML/CFT framework, as transactions would increasingly take place outside the oversight of EU regulators. Consequently, the framework would not only fail to achieve its intended objectives but would also erode the competitiveness of the EU's digital economy by pushing innovation and market leadership to jurisdictions with more balanced regulatory approaches.

The combined effect of these measures could hinder the EU's ambitions to position itself as a leader in digital finance, stifling innovation while imposing substantial compliance burdens on regulated entities. This highlights the need for a nuanced regulatory approach that considers the realities of open-source technologies and ensures a level playing field for European CASPs in the global economy.

3.3. AML Regulation (EU) 2024/1624[6]

This regulation will enter into force on 10 July 2027.

[6] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

The primary objective of the regulation to achieve a harmonised regulatory framework for AML and CFT, while simultaneously addressing emerging challenges arising from technological advancements. This framework introduces new and more stringent regulations pertaining to P2P transactions and transactions involving non-custodial wallets. The enforcement of these regulations will necessitate the imposition of additional obligations on obliged entities, which will include:

1. Obligation to implement proportionate measures and procedures, which shall include an assessment of the risks associated with transactions involving non-custodial wallets.
2. Prohibition on the maintenance of anonymous or anonymity-enhancing accounts, including crypto-assets that facilitate anonymity (with the exception of hardware and software providers or non-custodial wallet providers under the condition that they do not have access to or control over such wallets).
3. Obligation to identify and assess the risks associated with the use of non-custodial wallet addresses, recognising that the utilisation of a non-custodial wallet may indicate a potentially heightened risk.
4. Obligation to implement additional measures concerning transactions involving non-custodial wallets, which shall include: (1) identification and verification of the identity of the parties involved; (2) the collection of supplementary information regarding the origin and destination of the crypto-assets; (3) enhanced ongoing monitoring of transactions associated with non-custodial wallet addresses; and (4) any other measures aimed at mitigating the risk of money laundering.
5. Obligation to report to the Financial Intelligence Unit (FIU) on their own initiative when the obliged entity knows, suspects, or has reasonable grounds to suspect that funds or activities, irrespective of the amount involved, are the proceeds of criminal activity or are linked to terrorist financing or other criminal activities. The obliged entity shall provide the FIU with all necessary information, including transaction records, without the need for prior approval from an independent authority. Important note: By July 10, 2027, the Authority for Anti-Money Laundering ("AMLA") is required to issue guidelines to specify the mitigating measures referred to the above.

As a new development, these obligations shall also be applicable to crowdfunding intermediaries, specifically providers of crowdfunding platforms that facilitate the organisation of fundraising campaigns, including those pertaining to humanitarian aid, as well as the processing of donations, including in the form of crypto-assets.

3.4. AML Directive (EU) 2024/1640[7]

In conjunction with AML Regulation (EU) 2024/1624, this Directive constitutes a comprehensive package aimed at reinforcing the European Union's AML and CFT framework. It is set to replace Directive 2015/849 with more stringent regulations, mandating that Member States and private entities implement enhanced measures for risk identification, transparency, and improved cooperation among regulatory bodies.

[7] AML Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849.

Key developments include:

1. The obligation for each Member State to establish a Financial Intelligence Unit (FIU) responsible for receiving and analysing reports submitted by obligated entities. In practice, this entails that FIU personnel will have access to all financial data collected by obligated entities regarding their clients.
2. The obligation for each Member State to designate a fundamental rights officer. This officer is tasked with ensuring that the FIU adheres to fundamental rights, providing guidance, and overseeing its legal and ethical practices without impeding its operations. Important note: In practice, the officer lacks the necessary tools to exert real influence over the FIU's activities in cases of fundamental rights violations.
3. The authority of the Anti-Money Laundering Authority (AMLA) to subject crypto-asset service providers to special oversight may pose a risk of the AMLA exerting pressure on providers to decline transactions originating from non-custodial wallets.

Member States are required to adopt the laws, regulations, and administrative provisions necessary to comply with this Directive by July 10, 2027.

4. FINANCIAL ACTION TASK FORCE GUIDELINES

The Financial Action Task Force (FATF) is an intergovernmental organisation established in 1989 by the G7 to develop and promote policies aimed at combating money laundering and the financing of terrorism. As a global standard-setting body, FATF issues guidelines and recommendations that member countries are encouraged to implement to enhance their AML and CFT frameworks.

In addressing the issues of non-custodial wallets and peer-to-peer (P2P) transactions, FATF recognizes the unique risks associated with these technologies. Non-custodial wallets, which allow users to control their own private keys and funds without relying on a third party, can obscure the identities of individuals involved in transactions and the origins of funds. Similarly, P2P transactions, which occur directly between users without intermediaries, are not subject to the same AML/CFT controls as transactions facilitated by regulated entities.

FATF's approach emphasizes a risk-based methodology, urging countries to assess and mitigate the risks posed by these technologies. While P2P transactions are not directly regulated under FATF standards, the organisation encourages member states to implement measures that enhance transparency and oversight of virtual asset service providers (VASPs) and to develop tools for monitoring P2P activities. This includes the use of blockchain analytics to identify and assess risks associated with non-custodial wallets and to ensure that appropriate controls are in place to prevent illicit activities. Through these efforts, FATF aims to strengthen the global response to financial crime while adapting to the evolving landscape of digital assets.

The following points summarise FAFT’s approach towards non-custodial wallets and peer-to-peer transactions:

1. The guidelines highlight that the use of non-custodial wallets can obscure the identities of individuals involved in transactions and the origin or destination of funds. This is identified as a red flag for potential money laundering and terrorist financing activities.

2. The guidelines specify that P2P transactions are not subject to AML/CFT controls under FATF standards, as the obligations are placed on intermediaries rather than individuals. This indicates a regulatory gap concerning direct transactions between individuals.
3. The guidelines outline risk factors associated with virtual assets, including the use of non-custodial wallets. It notes that transactions involving non-obliged entities (e.g., non-custodial wallets) and prior P2P transactions may present heightened risks.
4. FATF recommends that countries develop methodologies and tools, such as blockchain analytics, to assess P2P market metrics and risk mitigation solutions. This includes determining whether wallets are hosted or self-hosted, which relates to the use of non-custodial wallets.
5. The guidelines suggest implementing measures for ongoing risk-based enhanced supervision of VASPs and controls to facilitate visibility of P2P activity. This includes requiring VASPs to only facilitate transactions to and from addresses that have been deemed acceptable, which may involve scrutiny of non-custodial wallet transactions.

Overall, the FATF emphasizes the risks associated with non-custodial wallets and P2P transactions, while also outlining the regulatory challenges and recommendations for addressing these risks within the AML/CFT framework.

5. POTENTIAL COLLISION OF AML AND CFT REGULATIONS WITH THE RIGHT TO FINANCIAL PRIVACY

The aforementioned AML and CFT regulations mandate CASPs to gather extensive customer data related to transactions involving non-custodial wallets, including both transfers sent to such wallets and those received from them. This includes, among other things, names and addresses of the originator and beneficiary of the transaction, and their wallet addresses. Upon request from member state authorities responsible for combating money laundering and terrorist financing, CASPs are obliged to disclose this data. Granting such access to financial data may constitute an unacceptable interference with the customers' right to financial privacy.

The right to privacy is a fundamental human right aimed at protecting individuals from excessive interference by public authorities in their private lives. It encompasses private and family life, the confidentiality of correspondence, and the protection of financial data, including information about non-custodial wallet addresses, owned crypto-assets, and transaction histories. This right is enshrined in Article 12 of the Universal Declaration of Human Rights, Article 8 of the European Convention on Human Rights, and Article 7 of the Charter of Fundamental Rights of the European Union.

Any interference with the right to privacy, according to Article 52 of the Charter of Fundamental Rights, is permissible only if it meets strict conditions: (1) it must be based on law (in the EU, this typically means a regulation or directive), (2) it must respect the essence of the right to privacy, (3) it must be proportionate to the objective pursued, and (4) it must be necessary and genuinely meet objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.

The jurisprudence of the Court of Justice of the European Union ("**CJEU**") has further established two cumulative conditions for lawful interference with the right to privacy:

1. it must relate to specific individuals suspected of planning, committing, or having committed serious crimes in the context of ongoing proceedings, and

2. access must be subject to prior authorization by an independent body, such as a court, based on a justified request from a public authority within a criminal investigation.

The AML and CFT regulations do not define detailed procedural requirements for accessing customer financial data but instead delegate this responsibility to member states. Numerous CJEU rulings indicate that procedures established by member states often fail to meet these conditions and conflict with Article 52 of the Charter. Criticisms include the lack of prior judicial or independent oversight, insufficient independence of oversight bodies, excessive scope of data sharing, and the absence of a requirement for ongoing legal proceedings related to the data requested.

In conclusion, the AML and CFT regulations requiring CASPs to collect and disclose customer data to state authorities pose significant risks to the right to privacy. The absence of unified and precise procedural safeguards and the risk of improper implementation by member states, as highlighted in CJEU rulings, increase the likelihood of violations and the misuse of data for purposes unrelated to crime prevention, such as political objectives. While these regulations entail substantial intrusions into privacy, they fail to ensure adequate protection of CASP customers' private lives.

6. SOURCES

This report was prepared based on the following documents.

EU Directives

1. Directive (EU) 2013/36 of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.
2. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
3. Directive (EU) 2024/1619 of the European Parliament and of the Council of 31 May 2024 amending Directive 2013/36/EU as regards supervisory powers, sanctions, third-country branches, and environmental, social and governance risks.
4. Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849.
5. Directive (EU) 2024/1654 of the European Parliament and of the Council of 31 May 2024 amending Directive (EU) 2019/1153 as regards access by competent authorities to centralised bank account registries through the interconnection system and technical measures to facilitate the use of transaction records.

EU Regulations

6. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.
7. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
8. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
9. Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.
10. Regulation (EU) 2024/1623 of the European Parliament and of the Council of 31 May 2024 amending Regulation (EU) No 575/2013 as regards requirements for credit risk, credit valuation adjustment risk, operational risk, market risk and the output floor.

The EBA Guidelines

11. Final Report of 16 January 2024 – Guidelines amending Guidelines EBA/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; (EBA/GL/2024/01).
12. Final Report of 7 April 2024 – Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113; (EBA/GL/2024/11).
13. Final Report of 27 November 2023 – Guidelines amending Guidelines EBA/GL/2021/16 on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (The Risk-Based Supervision Guidelines); (EBA/GL/2023/07).

FATF Guidelines

14. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers of October 2021.
15. Report for Virtual Assets Red Flags Indicators of Money Laundering and Terrorist Financing of September 2020.
16. Procedures for the FATF AML/CFT/CPF Mutual Evaluations, Follow-Up and ICRG, FATF (2024).

17. Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems FATF (2013-2023).
18. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation FATF, (2012-2023).
19. Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectivenesss of AML/CFT/CPF Systems, FATF (2024).
20. Money Laundering National Risk Assessment Guidance, FATF (2024).
21. Virtual Currencies, Key Definitions and Potential AML/CFT Risks, FATF (2014).

Treaties

22. Charter of Fundamental Rights of the European Union (2012/C 326/02).
23. European Convention on Human Rights, Council of Europe, 1950.
24. Universal Declaration of Human Rights, Paris 10 December 1948.

Selected jurisprudence

25. Judgment of the Court of Justice of 8 April 2014, C-293/12, Digital Rights Ireland Ltd. vs. Minister for Communications, Marine snd Natural Resources and Others, and Kärntner Landesregierung And Others, ZOTSiS 2014, No. 4, p. I-238.
26. Judgment of the Court of Justice of 21 December 2016, C-203/15, Tele2 Sverige AB vs. Post-Och Telestyrelsen and Secretary of State for the Home Department vs. Tom Watson, Peter Brice and Geoffrey Lewis, ZOTSiS 2016, No. 12, p. I-970.
27. Judgment of the Court of Justice of 5 April 2022, C-140/20, G.D. vs. the Commissioner of the Garda Síochána and Others.

Other sources

28. "Building True Change (BTC) Coalition Submission on the EU Proposal for a Regulation on the prevention of money laundering or terrorist financing", Kozlovska L., Jardemalie B. (https://en.odfoundation.eu/a/725781,building-true-change-btc-coalition-submission-on-the-eu-proposal-for-a-regulation-on-the-prevention-of-money-laundering-or-terrorist-financing/)
29. "Submission to FATF: Tools to prevent abuse of AML/CFT laws", Kozlovska L., Jardemalie B. (https://en.odfoundation.eu/a/723329,submission-to-fatf-tools-to-prevent-abuse-of-aml-cft-laws/)