Baker McKenzie.

June 2025

MiCAR Compliance Toolkit

Anti-Money Laundering Requirements

Contents

Global regulators have long been concerned about the financial crime risks posed by the increasing use of crypto, particularly to launder illicit proceeds, in the absence of targeted rules on anti-money laundering and counter-terrorist financing (AML/CTF).

Several high profile money laundering cases involving crypto businesses in recent years have underscored the need for robust regulation to mitigate these risks. In response, EU lawmakers have closed the regulatory gaps through the Markets in Cryptoassets Regulation (MiCAR) and forthcoming reforms to the EU AML framework.

For an overview of key upcoming changes for financial institutions arising from the EU AML reform package, see our dedicated guide **here**

The Wire and Cryptoasset Transfer Regulation (WCTR) amended the Money Laundering Directive (MLD4) to apply the full set of AML/CTF requirements to cryptoasset service providers (CASPs) falling within scope of MiCAR, and revised and recast the Wire Transfer Regulation (WTR) to extend the regime for fund transfers to the transfer of cryptoassets. The WCTR repealed and replaced the WTR on 30 December 2024, taking effect at the same time as the application of MiCAR to CASPs. As a result, since 30 December 2024 the cryptoasset regime under MiCAR and the AML/CTF rules under the WCTR and MLD4 have been aligned, closing gaps that previously existed.

MLD4 requirements: The general AML regime

The existing AML/CTF regime set out in MLD4 applies to CASPs as it does to any other financial institution, with the exception of CASPs which only provide advice on cryptoassets. This means that CASPs within scope will need to:

- Carry out risk-based customer due diligence (CDD) and verification measures when entering into business relationships or carrying out occasional transactions above a certain threshold.
- Undertake enhanced due diligence (EDD) measures when establishing new correspondence relationships.
- Comply with suspicious activity and transaction reporting requirements.
- Establish internal policies, procedures and controls for risk assessment and AML compliance (including group-wide policies and procedures where applicable). The adequacy and effectiveness of those mechanism, systems and procedures must be monitored and evaluated on a regular basis, taking into account the scale, nature and range of cryptoasset services provided, and appropriate measures must be taken to address any deficiencies.

Under MLD4 (as amended by the WCTR), CASPs must also identify, assess and take mitigating measures associated with cryptoasset transfers to or from self-hosted addresses (i.e., self-hosted wallets). To achieve this, CASPs must have in place internal policies, procedures and controls.

WCTR requirements: The travel rule

The WCTR extends the "travel rule" for fund transfers to cryptoassets, aligning with changes to the Financial Action Task Force's international standards by ensuring that cryptoasset transfers can be traced for AML/CTF purposes. CASPs must ensure that information on the originator and beneficiary of cryptoasset transfers travels with the transfer through the payment chain and is retained at both ends of the transaction. Unlike fund transfers, the same obligations apply whether the cryptoasset transfer is domestic or cross-border, and there is no exemption for domestic low-value cryptoasset transfers.

The WCTR also supplements the AML/CTF obligations regarding self-hosted wallets. Where a cryptoasset transfer involves a self-hosted wallet, CASPs must obtain and hold information on the originator and beneficiary; where the transfer amount exceeds EUR 1,000, CASPS must take adequate measures to assess whether the self-hosted wallet is owned or controlled by the originator or beneficiary.

Further, the WCTR sets out a new requirement to establish internal policies, procedures and controls to ensure implementation of restrictive measures (i.e., sanctions) when performing cryptoasset transfers.

MiCAR requirements: Additional obligations

While MiCAR does not implement a bespoke AML/CTF regime for crypto businesses beyond the current MLD4 framework, there are provisions imposing certain additional requirements.

For example, CASPs and issuers of asset-referenced tokens (ARTs) applying for authorization must provide proof that that members of the management body and direct and indirect shareholders with qualifying holdings in the applicant have not been convicted of an AML/CTF offence. For applicant CASPs, information on AML/CTF internal controls and compliance must accompany the application for authorization: at the time of writing, draft Level 2 measures propose that the information to be submitted with the application for authorization must include a detailed description of the internal control mechanisms and procedures ensuring compliance with AML/CTF obligations. Applications may be refused if there are serious risks of money laundering or terrorist financing.

Additionally, for CASPs operating a trading platform, the admission approval processes set out in the platform operating rules must include CDD commensurate to the money laundering or terrorist financing risk presented by the applicant in accordance with the AML/CTF regime that are applied before admitting the cryptoassets to trading. CASPs operating a trading platform must also prevent the admission to trading of cryptoassets that have an inbuilt anonymization function, unless the CASP can identify the holders of those cryptoassets and their transaction history.

The EU AML reform package: Key changes

There are a number of changes set out in the EU AML reform package that strengthen the current AML/CTF requirements applying to CASPs. These include:

- Substantially lowering CDD thresholds for cryptoasset transactions as compared to other financial transactions. CASPs will need to apply CDD measures when carrying out cryptoasset transactions with a value of at least EUR 1,000. For all cryptoasset transactions, CASPs will need to at least identify the customer and verify their identity.
- Extending the prohibition on anonymous bank accounts and safe-deposit boxes to include anonymous cryptoasset accounts as well as any account otherwise allowing for the anonymization of the customer account holder or the anonymization or increased obfuscation of transactions, including through "anonymity-enhancing coins". This aligns with the prohibition in MiCAR on trading platforms admitting cryptoassets that have an inbuilt anonymization function, as noted earlier.
- Expanding the information included in bank account registers to include cryptoasset accounts as well as virtual IBANs and securities accounts, in addition to the existing mandated information on payment accounts, bank accounts and safe-deposit boxes.
- Including CASPs within the pool of financial institutions that could be subject to direct supervision by the new EU AML/CTF regulator, AMLA.

Key contacts

United Kingdom

Mark Simpson
Partner
Mark.Simpson
@bakermckenzie.com

Melody Hoay
Associate
Melody.Hoay
@bakermckenzie.com

Sarah Williams
Associate
Sarah.Williams
@bakermckenzie.com

Kimberly Everitt
Senior
Knowledge Lawyer
Kimberly.Everitt
@bakermckenzie.com

Austria

Robert Wippel
Counsel
Robert.Wippel
@bakermckenzie.com

Belgium

Olivier
Van den broeke
Associate
Olivier.Vandenbroeke
@bakermckenzie.com

Czech Republic

Jan Kolar
Associate
Jan.Kolar
@bakermckenzie.com

France

Iris Barsan
Counsel
Iris.Barsan
@bakermckenzie.com

Elisa Deuffic
Associate
Elisa.Deuffic
@bakermckenzie.com

Germany

Manuel Lorenz
Partner
Manuel.Lorenz
@bakermckenzie.com

Conrad Ruppel
Partner
Conrad.Ruppel
@bakermckenzie.com

Manuel Metzner
Counsel
Manuel.Metzner
@bakermckenzie.com

Hungary

József Vági
Partner
Jozsef.Vagi
@bakermckenzie.com

Italy

Eugenio Muschio
Partner
Eugenio.Muschio
@bakermckenzie.com

Luxembourg

Catherine Martougin
Partner
Catherine.Martougin
@bakermckenzie.com

Netherlands

Tim Alferink
Partner
Tim.Alferink
@bakermckenzie.com

Willem van Rees
Associate
Willem.vanRees
@bakermckenzie.com

Poland

Jerzy Bombczynski
Counsel
Jerzy.Bombczynski
@bakermckenzie.com

Spain

Paula De Biase
Partner
Paula.DeBiase
@bakermckenzie.com

Javier Portillo
Associate
Javier.Portillo
@bakermckenzie.com

Berta Satrustegui
Associate
Berta.Satrustegui
@bakermckenzie.com

Switzerland

Yves Mauchle
Partner
Yves.Mauchle
@bakermckenzie.com

Ansgar Schott
Partner
Ansgar.Schott
@bakermckenzie.com

Check out the other guides in our **MiCAR Compliance Toolkit**

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com