Fireblocks®

CHEAT SHEET

# How to prepare your business for upcoming MiCA and DORA regulations

In the cryptocurrency and digital asset space, regulations can change rapidly and vary widely from region to region. In the EU, two new regulatory rulebooks will come into effect soon: the Markets in Crypto-Assets Act (MiCA) in Q4 2024 and the Digital Operations Resilience Act (DORA) in Q1 2025.

With these new regulations on the horizon, there is an opportunity for greater clarity on how industry players should conduct their businesses – representing the potential for a uniquely secure and transparent crypto environment in the EU. At the same time, as these rules come into effect, there are many key points to consider for entities working with digital assets in the EU, and ensuring compliance with these regulations will be of vital importance for many businesses.

We compiled this compliance cheat sheet on MiCA and DORA to help EU-based businesses prepare for these new requirements. Read on to learn how MiCA and DORA function, and what these new rules could mean for your business.

## The Basics

### What is MiCA?

MiCA is a regulation adopted by the EU. While some rules, like those on issuing stablecoins, have already been in effect since June 2024, harmonized rules for crypto-asset service providers will start to apply as of 30 December 2024. Transition periods may vary depending on the nature of the crypto activity and where it is primarily conducted. However, most regulated entities will have 18 months to achieve compliance.

MiCA provides a new licensing regime for crypto-asset service providers ("CASPs") and crypto-asset issuers. CASPs are simply new or existing businesses that offer certain crypto-asset services to clients on a professional basis. Specifically, there are five categories of services that require registration under MiCA:

1. Custody or administration services
2. Operating an exchange
3. Investing or trading crypto-assets on behalf of others
4. Advising on crypto asset portfolio management on behalf of others
5. Payments services

Under MiCA, CASPs will have to comply with regulations that we often associate with traditional financial institutions, like rules on stability, custody, or market integrity. Being licensed under MiCA also brings these entities under Europe's AML rules, like KYC requirements. MiCA also regulates the issuance of crypto assets as Asset Referenced Tokens (ARTs) or Electronic Money Tokens (EMTs), as well as all utility tokens. Helpfully, it resolves the debate on whether a token is a security or not. The types of tokens defined in MiCA are not securities.

### What is DORA?

DORA is a directive adopted by the EU. It applies from 17 January 2025. The objective of DORA is to harmonize the risk management practices of financial institutions and their use of information communication technologies ("ICT") and third party information communication technology service providers ("ICT TPP"). DORA provides a common set of technology outsourcing requirements for financial institutions in the EU.

DORA established an oversight framework that requires all financial institutions (including CASPs) to comply. Under DORA, certain services providers designated as "critical" by the pan-European authorities will also be regulated and subject to certain compliance requirements and enforcement mechanisms.

## Best practices for meeting new regulatory requirements

### 1. Identify your obligations

In order to assure compliance with these new regulations, it is first important to establish whether or not your business is subject to them. Remember, it's important to conduct your own legal analysis (including potentially seeking legal advice) as you work toward MiCA and DORA compliance. That said, set out below is a brief summary of obligations set out in these regulations.

#### MiCA: Are you subject to the regulation?

First, you should identify if you are a Crypto Asset Provider or a Crypto Asset Issuer operating in or serving customers within the EU. These are the entities that are subject to the MiCA regulation. CASPs are:

- ☑ Any operators of trading platforms for crypto-assets, i.e., a central digital asset or crypto exchange (CEX)) (Article 3(1) no. 18)
- ☑ Anyone providing custody and administration of crypto-assets on behalf of clients, i.e., a qualified custodian (QC) (Article 3(1) no. 17)
- ☑ Anyone engaged in exchange of crypto-assets for funds or other crypto-assets: (Article 3(1) no. 19 and 20)
- ☑ Anyone executing orders for crypto-assets on behalf of clients, such as Market Makers, Traders, (Article 3(1) no. 21)
- ☑ Anyone receiving and transmitting orders for crypto-assets on behalf of clients, such as broker/dealers, prime brokers, (Article 3(1) no. 23)
- ☑ Anyone providing transfer services for crypto-assets on behalf of clients, like transfer agents, (Article 3(1) no. 26)
- ☑ Others:
  - ☑ Providing advice on crypto assets (Article 3(1) no. 24)
  - ☑ Placing of crypto assets: means the marketing on behalf of an offeror (Article 3(1) no. 22)
  - ☑ Portfolio management of crypto assets: managing portfolios in accordance with mandates given by clients on a discretionary client-by-client basis where such portfolios include one or more crypto-assets (Article 3(1) no. 25).

MiCA stipulates licensing requirements, in addition to conduct of business requirements, for each type of CASP. Broadly speaking, to get licensed you must be able to answer the following questions:

- ☑ Can you demonstrate financial soundness and meet capital requirements? Under MiCA that means:
  - — A permanent minimum capital requirement that varies from 50,000 to 150,000 Euros, depending on the type of the crypto-asset service provided (Article 67(1)(a) and Annex IV)
  - — Safeguards equal to one quarter of the fixed overhead of the preceding year (if such amount is higher than the permanent minimum capital) (Article 67(1)(b))
- ☑ Is your management team fit for governance?
  - — The governance requirements include the suitability requirements that apply to members of the management body (Article 68(1))
- ☑ Do you have governance systems in place for AML/KYC?
  - — You must have effective systems, procedures and arrangements to detect and prevent money laundering and terrorist financing (Article 68(8)).
- ☑ Are you already regulated under MiFID?
  - — If you firm is a regulated entity under MiFID such as a credit institution, investment firm, UCITS manager, or other type, and you plan to provide certain types of crypto asset services, you'll need to notify the competent authority at least 40 days before providing those services (Article 60(1) (5)).

MiCA also sets out requirements for asset-issuers:

- [x] Are you issuing a stablecoin?
  - For issuers of Utility Tokens, Asset-Referenced Tokens (ARTs) or E-Money Tokens, there are specific requirements around disclosure, financial reserve requirements, as well as redemption and recovery plans.
    - In keeping with the ethos of MICA to protect and empower investors as well as to ensure a resilient and efficient market, you should consider governance around
      1. Security controls
      2. Capital and risk management
      3. Auditability

**DORA: Are you subject to the regulation?**

First, businesses that are  subject to DORA, fall into the categories outlined in Article 2 of the regulation, but if your business qualifies as a CASP or is an issuer of asset-referenced tokens under MICA, you will be subject to DORA.

Second, if you are a DORA-regulated entity, you must assess if your ICT providers meet particular standards, set out in Article 30 of DORA. If they support functions that you, the regulated entity, deem "critical," your ICT providers need to meet additional enhanced requirements in their contracts.

## 2. Perform a gap analysis

As you prepare for MiCA compliance, it's important to review your business model and your governance systems, as well as consider if your risk management controls are well-documented, integrated into your workflows, and scalable to fit your business.

When thinking about how your governance will stack up, you may want to consider the following:

- [x] Are you able to custody across jurisdictions and manage assets across hot, warm, and cold wallets?
- [x] How are you mitigating counterparty risk, managing collateral, and managing post-trade and settlement?
- [x] Do you have a multi-layer security approach in place to protect against external and internal threats as well as disaster recovery plans that safe-guard assets?
- [x] Do you have compliance controls for all actions/transactions that are automated and embedded into workflows?
- [x] Do you have clearly documented and secure governance policies that are flexible and scalable?
- [x] Do you have a clear view of assets and reserves that are auditable?
- [x] As you consider operating in the EU or beyond, do you have systems in place that allow you to easily scale transactions, volumes, and customers without compromising security or compliance controls?

Under DORA, it's important to:

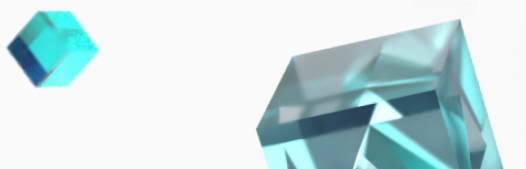
- [x] Determine the vendors that support your critical functions
- [x] Ask your vendors to provide:
  - Audits & Certifications
  - Information security and internal security policy and procedure documentation
  - Third-party risk management
  - Incident and vulnerability monitoring, response and management
  - Identity and access management
  - Product and code assurance practices
- [x] Audit your key management, governance, and access for any points of security compromise

## 3. Set Controls: What does it look like in practice?

What should compliant practices look like within your tech stack and throughout your organization?

**MiCA**

- [x] Secure and scalable governance management with the ability to configure policies and security based on organizational structure (and jurisdiction, if you are operating in multiple markets) at scale



- [x] Transaction screening tools and embedded sanctioned wallet blocking to meet AML, KYC and Travel Rule requirements.
  - Transaction screening, prior to signing transactions
- [x] Secure counterparty risk and collateral management
- [x] Automations to allow for:
  - Transaction screening, integrated into your transaction flow
  - Sweeping and settlement to a custodial accounts, across multiple markets
- [x] Multiple, segregated vault accounts to allow for customizable governance
- [x] Auditability for stablecoin issuers
  - Transparent, auditable ledger of assets and reserves
  - You're able to clearly provide documentation of reserves as well as embedded governance and controls

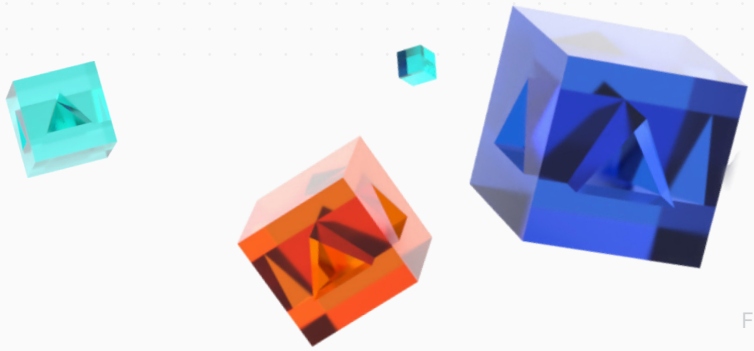
**DORA**

- [x] Know your ICT providers that support critical functions in your organization:
  - Review their information security, risk & vulnerability management, Third Party Risk Management (TPRM), incident management, service monitoring (SRE, customer operations), identity & access management, product and code assurance practices
  - Set up regular reporting in order to ensure up-to-date information about code, vulnerabilities and patches, etc.
- [x] Have a multi-layer security strategy for key management that includes hardware security and no single point of compromise, using threshold cryptography/MPC

## How Fireblocks supports MiCA and DORA compliance

Fireblocks supports compliance with MiCA via tools that can help organizations adhere to the regulations, as well as with DORA, as we function as a CTPP.

- [x] Customizable, tamper-proof, self-service governance management
  - The Fireblocks Policy Engine gives you the ability to configure policies and security based on organizational structure, ensuring that required user access and approvals are met before every transaction is executed with automated or manual authorization workflows.
- [x] Transaction screening tools integrated into your transaction flow
  - Automated transaction screening and embedded sanctioned wallet blocking are natively integrated into your transaction flow to help you meet requirements under the EU AML Rules, KYC obligations, and Transfer of Funds Regulation (aka Travel Rule), even at large volumes.
- [x] Full control of capital in trading activities to meet risk mitigation requirements
  - Through Fireblocks Off-Exchange, achieve faster settlement, simpler dispute resolution, and more transparent collateral management across trading activities. With Fireblocks' unique design, you don't just transfer counterparty risk – you eliminate it entirely.
- [x] Management of qualified custodial accounts from a single dashboard
  - Automations allow you to sweep funds and settlement to custodial accounts or cold storage across multiple markets, all within the Fireblocks Platform.
- [x] Segregation of funds
  - Multiple, segregated vault accounts empower customisable governance.
- [x] Control & auditability for regulated stablecoin issuers
  - Transaction monitoring, risk assessment tools, workflow authorisation for risk mitigation, and audit access built around MiCA compliant smart contracts ensure complete stablecoin compliance.



## DORA: Fireblocks as a third-party provider

Fireblocks works with over 2,000 institutions globally, including major financial institutions regulated within the EU. We have engaged with various national competent authorities regarding our service offering, including participating in audits of our customers conducted by European regulators.

**Fireblocks' approach to security:**

- **Security at the Core**: Defense-in-depth architecture combines MPC-CMP and hardware security to eliminate single point of compromise and create a secure environment for storing, issuing, and transferring digital assets.
- **Battle-tested Performance**: Our infrastructure is reliable and resilient at scaling the most demanding use cases that require millions of wallets and high transaction throughput.
- **Flexible Deployment Models**: Deploy the Fireblocks platform to your business requirements with SaaS, Private Cloud or On-Prem options, leveraging MPC, Secure Enclave or HSM for key management. Fireblocks now supports Azure, AWS, GCP, and Alibaba Cloud.
- **Multi-Blockchain Support**: Fireblocks' node and wallet infrastructure provides out of the box support for 50+ blockchains and the leading token standard such as ERC, SPL, XRPL, and more, with extensible support for any public or private EVM.

Fireblocks is the only security platform that insures assets in storage and in transfer. Fireblocks is SOC 2 Type II certified and completes regular pen testing from ComSec and NCC Group. We are also the first crypto tech company to be certified by the International Organization for Standards in security (ISO 27001), cloud (ISO 27017) and privacy (ISO 27018).

**Disclaimer: Please note this article is prepared for the general information of interested persons and it does not contain nor provide legal advice. Fireblocks encourages you to conduct your own analysis (including seeking independent legal advice) with respect to the applicability of MiCA and DORA on your business or operations.**