HACKEN

CASP/VASP Licensing & Compliance Handbook

Your path to MiCA, DORA
& EU approval

hacken.io

Inside the New EU Crypto Framework

As of 2025, the European Union has enacted groundbreaking regulations that have reshaped the crypto industry. The Markets in Crypto-Assets (MiCA) Regulation and the Digital Operational Resilience Act (DORA) are now in force, ushering in a new era of compliance for all crypto businesses, from centralized exchanges to DeFi platforms.

Why it matters: Non-compliance is not an option. Firms face stringent new obligations and heavy penalties. For example, DORA violations can trigger fines of up to €5 million or a significant percentage of annual turnover, and even the suspension of licenses. This handbook is designed to help you navigate these requirements with confidence.

MiCA Deep Dive

The Markets in Crypto-Assets Regulation (MiCA) is a landmark EU-wide law that establishes a unified framework for crypto-asset markets. Adopted in 2023, it is the world's first comprehensive attempt to regulate crypto-assets across all 27 EU member states, covering everything from Bitcoin and utility tokens to stablecoins.

Purpose: MiCA aims to protect consumers and ensure market integrity without stifling innovation. It brings clarity and accountability by requiring CASPs to obtain a license, holding exchanges liable for customer losses, and mandating transparency through measures like white papers for token offerings. It also imposes strict oversight on stablecoin issuers to ensure they maintain adequate reserves.



Timeline: MiCA is rolling out in phases:

June 2024

Rules for stablecoins (asset-referenced tokens and e-money tokens) began to apply.

December 30, 2024

The main CASP licensing regime kicked in. From 2025 onward, any company providing crypto-asset services in the EU must be authorized under MiCA.

Global Impact

MiCA is being watched worldwide and may serve as a model for other jurisdictions. This "Brussels Effect" means that achieving MiCA compliance is not just a key to the EU market but a strategic investment in future-proofing a firm's global operations.

CASP Licensing: How to Get Authorized Under MiCA

Who needs a license

If your business provides any of the following services to clients in the EU, you must obtain a CASP license:

- Custody and administration of crypto-assets
- Operation of a trading platform
- Exchange of crypto-assets for fiat or other crypto-assets
- Execution of orders
- Placing of crypto-assets
- Providing advice or portfolio management on crypto-assets
- Transfer services for crypto-assets

The license process

A firm must apply to its National Competent Authority (NCA)—such as BaFin in Germany, FMA in Austria or AMF in France—with a comprehensive dossier of documents. Regulators will conduct a thorough assessment of the application, including the suitability of management and shareholders.

Getting a license is not just about paperwork; it requires a company to be fully prepared to operate under regulatory oversight. Firms should conduct internal readiness assessments to identify and address gaps before applying.

Several major entities have taken significant steps to align with the EU's regulatory framework, including securing national registrations or MiCA licenses in key jurisdictions:

- **Binance**
  Updated its operations in Poland with stricter AML controls and full user verification under the national VASP regime.
- **Bybit**
  Secured a MiCA license from Austria's FMA, allowing Bybit to operate as a regulated crypto provider in the EEA.
- **Bitpanda**
  Secured a MiCA license in Germany, enabling regulated trading and custody services.
- **Boerse Stuttgart Digital**
  Became the first German entity to receive a MiCA license, expanding its regulated crypto services.
- **Crypto.com**
  Received approval to operate under MiCA across multiple EU countries, focusing on compliant trading services.
- **MoonPay**
  Licensed under MiCA to provide crypto payment processing while adhering to AML standards.
- **OKX**
  Secured a MiCA license in France, enabling the company to offer regulated spot trading, custody, and crypto-to-fiat services across the EU.
- **Kraken**
  Secured a MiCA license from Ireland's central bank to operate its European business under a unified regulatory framework.
- **Coinbase**
  Obtained its MiCA license via Luxembourg, enabling passporting rights to serve EU customers under a single regulatory regime.

Passporting Rights: One License, Whole Europe

One of MiCA's most powerful advantages is "passporting." Once a CASP license is obtained, it becomes valid across all 30 countries — the 27 EU member states plus Iceland, Liechtenstein, and Norway. This eliminates the need for separate licenses in each jurisdiction, making MiCA a true game-changer for scaling crypto businesses across Europe.

The notification process: To use passporting rights, a CASP simply notifies its home regulator of its intent to operate in other member states. The home regulator then informs the authorities in the host countries.

Strategic jurisdiction choice: The choice of where to apply for a license is critical. Factors to consider include the regulator's experience, the local business environment, and national transition timelines.

Pro-Innovation hubs	France is known for its pro-innovation stance and has a simplified transition process for existing providers.
Established financial centers	Germany offers a strong financial ecosystem but may have stricter supervisory scrutiny.
Agile jurisdictions	Lithuania and Estonia are known for being nimble and crypto-friendly, though requirements are tightening. Malta has also positioned itself as a key crypto hub, having already licensed CASPs under MiCA.

For non-EU firms: Companies based outside the EU cannot service EU clients without a MiCA license. They must establish a legal entity in an EU member state to apply for authorization. Relying on the narrow "reverse solicitation" exemption is a high-risk strategy, as regulators interpret it very strictly.

MiCA National Implementation Dashboard

Disclaimer: The implementation of MiCA across the European Union is a dynamic and ongoing process. The transitional ("grandfathering") periods and specific national requirements are subject to change based on the final enactment of domestic legislation and guidance from National Competent Authorities (NCAs). Firms must verify all information directly with the relevant NCA before making any strategic decisions.

The key advantage of MiCA is the creation of a single market for crypto-asset services. However, the path to this harmonized state involves a fragmented transition. While MiCA allows for a default 18-month grandfathering period for existing providers (ending July 1, 2026), many member states have exercised their right to shorten this period to accelerate the adoption of MiCA's stricter standards. A firm's compliance timeline is therefore dictated by the shortest transition period of any EU country in which it has clients.

EU Member State	National Competent Authority (NCA)	Status of National Implementing Law	Transitional Period Ends	Key Nuances & Application Deadlines
Austria	Financial Market Authority (FMA)	Implemented	Dec 31, 2025	Shortened 12-month period. All CASPs must be FMA-authorized to operate after this date.
Belgium	Financial Services and Markets Authority (FSMA)	Implemented	Jul 1, 2026	Full 18-month period adopted.
Bulgaria	Financial Supervision Commission (FSC)	Implemented	Dec 30, 2025	Shortened 12-month period. FSC designated as primary supervisor.
Croatia	Croatian National Bank (HNB) & Financial Services Supervisory Agency (HANFA)	Implemented (MiCA Implementation Act)	Jul 1, 2026	Full 18-month period. HNB and HANFA share supervisory duties.
Cyprus	Cyprus Securities and Exchange Commission (CySEC)	Implementation in progress, expected by end of 2024	Jul 1, 2026	Full 18-month period. No new national VASP applications are being accepted

Czech Republic	Czech National Bank (CNB)	Implemented (Act on the Digitalisation of the Financial Market)	Jul 1, 2026	Full 18-month period, but existing providers must apply for a MiCA license by Jul 31, 2025, to benefit from it.
Denmark	Danish Financial Supervisory Authority (DFSA)	Implemented	Jul 1, 2026	Full 18-month period, but firms must have applied by Dec 30, 2024, to benefit. DFSA has published application forms.
Estonia	Financial Supervision and Resolution Authority (ESFRA)	Implemented	Jul 1, 2026	Full 18-month period. Estonia's previous VASP regime was a model for MiCA.
Finland	Financial Supervisory Authority (FIN-FSA)	Implemented	Jun 30, 2025	Shortened 6-month period, one of the shortest in the EU. FIN-FSA has received 8 applications as of early 2025.
France	Autorité des Marchés Financiers (AMF) & Autorité de Contrôle Prudentiel et de Résolution (ACPR)	Implemented	Jul 1, 2026	Full 18-month period. Simplified "fast-track" procedure available for existing registered/licensed DASPs.
Germany	Federal Financial Supervisory Authority (BaFin)	Implemented (KMAG & FinmadiG)	Dec 31, 2025	Shortened 12-month period. A simplified procedure is available for certain existing BaFin-licensed entities.
Greece	Hellenic Capital Market Commission (HCMC) & Bank of Greece	Implemented	Dec 31, 2025	Shortened 12-month period
Hungary	Central Bank of Hungary (MNB)	Implemented	Jun 30, 2025	Shortened 6-month period. Foreign providers must comply with local AML rules during transition.
Ireland	Central Bank of Ireland (CBI)	Implemented	Dec 30, 2025	Shortened 12-month period. Existing VASPs must apply for a full MiCA license; no simplified procedure as VASP status is a registration, not an authorization.
Italy	CONSOB & Bank of Italy	Implemented (Legislative Decree 129/2024)	Dec 30, 2025	Shortened 12-month period. Critically, existing VASPs must apply by Jun 30, 2025, or cease operations.
Latvia	Bank of Latvia	Implemented	Jun 30, 2025	Shortened 6-month period.
Lithuania	Bank of Lithuania	Implemented	Jan 1, 2026	Extended transition period. Initial proposal for a 5-month period was revised. Firms can operate under old rules if they apply for a MiCA license by the new deadline.
Luxembourg	Commission de Surveillance du Secteur Financier (CSSF)	Implemented	Jul 1, 2026	Full 18-month period adopted for existing registered VASPs.
Malta	Malta Financial Services Authority (MFSA)	Implemented (Markets in Crypto-Assets Act)	Jul 1, 2026	Full 18-month period. Malta has positioned itself as a key crypto hub with a proactive regulator.
Netherlands	Authority for the Financial Markets (AFM) & De Nederlandsche Bank (DNB)	Implemented	Jun 30, 2025	Shortened 6-month period. AFM warns the application process takes 5-6 months and urges prompt submission.

Poland	Komisja Nadzoru Finansowego (KNF)	Draft Act pending, status is FLUID.	Jun 30, 2025 (Official) / Potentially later (Practical)	Highly uncertain. The official 6-month period is challenged by legislative delays. Recent proposals suggest a 4-month period after the national law is enacted. Previous application deadlines are likely invalid.
Portugal	Not yet formally defined	Draft Act pending	TBA	Significant legal uncertainty due to delays in passing national law and designating the NCA.
Romania	Financial Supervisory Authority (ASF) & National Bank of Romania (BNR)	Draft ordinance in consultation	Jul 1, 2026	Full 18-month period. ASF is the primary supervisor for CASPs.
Slovakia	National Bank of Slovakia (NBS)	Implemented	Dec 31, 2025	Shortened 12-month period.
Slovenia	Securities Market Agency (ATVP)	Implemented (Zakon o trgih kriptosredstev)	Jun 30, 2025	Shortened 6-month period.
Spain	Comisión Nacional del Mercado de Valores (CNMV) & Bank of Spain	Implemented	Dec 31, 2025	Shortened 12-month period. CNMV supervises CASPs; Bank of Spain supervises stablecoin issuers.
Sweden	Hellenic Capital Market Commission (HCMC) & Bank of Greece	Implemented	Dec 30, 2025	Shortened 9-month period. No simplified procedure will be used.

^Note: This table reflects the latest available information as of Q2 2025. Always verify with the respective National Competent Authority.

DORA at a Glance

The Digital Operational Resilience Act (DORA) is a new EU regulation that complements MiCA by focusing on ICT security and operational continuity. Effective January 17, 2025, DORA establishes a unified framework to ensure financial entities, including CASPs, can withstand, respond to, and recover from all types of cyber threats and ICT disruptions.

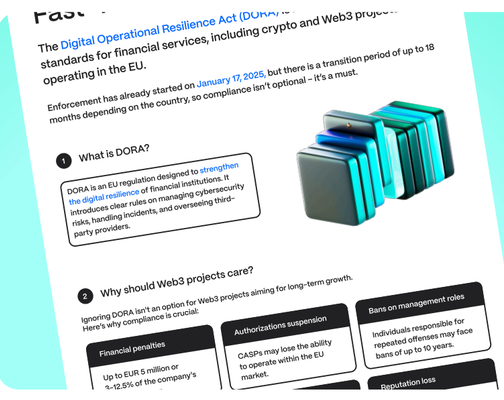
Who must comply: DORA applies to a broad range of financial entities, explicitly including CASPs authorized under MiCA. It also extends to critical third-party technology providers, such as cloud services.

Core objectives:

- Harmonize resilience standards across Europe.
- Prevent incidents through better risk management and ensure strong recovery plans.
- Increase oversight of critical third-party providers to reduce systemic risk.
- Bolster trust and stability in the entire financial system.

DORA & MiCA interplay: For CASPs, MiCA and DORA are inseparable. A firm cannot be MiCA-compliant without also being DORA-compliant. DORA provides the mandatory technical foundation upon which every CASP's operations must be built.

DORA Requirements	Key Components	Description
ICT Risk Management	• Assets Discovery, Threat Modeling, Risk Identification and Assessment • Protection, Detection, and Response • Risk Management Documentation Coverage	**Implement frameworks to identify, assess, and mitigate ICT-related risks proactively.** Examples: • Create a comprehensive inventory of Web2 and Web3 assets. • Evaluate the impact of Web2 and Web3 assets • Prioritize risk mitigation controls based on the assets business value. • Maintain a real-time dashboard showing all wallets and funds. • Review exposure to DeFi exploits and smart contract vulnerabilities.
Incident Reporting	• Incident Response, Business Continuity, and Disaster Recovery Processes • Recovery Action Plans • Structured Reporting • Accurate Submissions	**Establish clear protocols for detecting, classifying, and submitting ICT-related incident reports to regulators on time.** Examples: • Develop incident response plans and key compromise protocols based on the risk assessment outcomes for Web2 & Web3 assets. • Automate alerts for unusual wallet transactions. • Maintain backup nodes for uninterrupted access. • Set alerts for large or unusual token transfers. • Assess impact of a major liquidity event on business stability.
Digital Operational Resilience Testing	• Basic Testing • Advanced Testing	**Perform regular cyber resilience tests, including TLPT (Threat-Led Penetration Testing), to simulate real-world attacks and identify areas for improvement.** Examples: • Perform independent security assessment to identify security weaknesses in critical assets and underlying infrastructure e.g. Penetration Testing, Cloud Infrastructure Security Review, etc • Perform third-party auditing to identify potential exploits before deploying smart contracts. • Conduct Threat-Led Penetration Testing (TLPT) every 3 years with third-party experts. • Store treasury funds in a hardware wallet with multi-party approval.
ICT Third-Party Risk Management	• Monitoring and Oversight • Critical Provider Oversight	**Monitor and assess vendor compliance with ICT security standards, ensuring third-party systems meet regulatory expectations.** Examples: • Conduct due diligence to assess the compliance level of an exchange before storing funds. • Ensure the oracle has redundancy in place in case a primary data source fails. • Evaluate how a third-party service protects against private key leaks. • Ensure the provider has failover nodes in place to maintain 99.9% uptime



DORA compliance made easy: free checklist

Get your free checklist now and simplify your DORA compliance journey.

Chat with our experts now →

Top Questions About CASP/VASP Compliance

Q1: What is the actual deadline for obtaining a CASP license under MiCA?

A: For new businesses starting after December 2024, a license is required before beginning operations. For existing providers, there is a transitional "grandfathering" period, but the deadline varies by country, as detailed in the MiCA National Implementation Dashboard in this handbook. While some offer the full 18 months until July 1, 2026, others, like the Netherlands, have shortened it to mid-2025.

Q2: We already have a national crypto license (e.g., a French PSAN). Do we need to reapply under MiCA?

A: Yes. MiCA replaces national regimes. Existing licensees must obtain a MiCA authorization to operate beyond the transition period. However, many regulators, like those in France and Germany, are offering a simplified or "fast-track" conversion process for already registered firms.

Q3: Does MiCA or DORA apply to DeFi projects or NFT platforms?

A: This depends on the actual level of decentralization, and the answer is complex. MiCA states that it does not apply to crypto-asset services "provided in a fully decentralised manner without any intermediary," but this exemption is narrow and subject to intense regulatory scrutiny. The notion of a blanket "DeFi exemption" is a myth.

Regulators will perform a "substance-over-form" analysis to determine if an identifiable person or "undertaking" (a legal entity or a coordinated group) effectively controls the provision of a crypto-asset service. Key indicators of centralization that could bring a DeFi project into MiCA's scope include:

- **Governance control**
  Concentration of voting power in the hands of a small number of founders or investors.
- **Operational control**
  The existence of an entity that controls the primary user interface, holds administrative keys with the power to pause or modify smart contracts, or unilaterally controls the protocol's upgrade process.
- **DAO-adjacent entities**
  The presence of a foundation or company that employs core developers, manages the project's treasury, or conducts marketing for the protocol.

In conclusion, the "decentralization" exemption is not a wide-open door. Any project with an identifiable core team, a controlling foundation, or centralized technical components should assume it is likely within MiCA's scope and seek expert legal advice.

Q4: We are a non-EU company. Can we just geo-block EU users and avoid these rules?

A: Technically, yes. If you completely and effectively exclude all EU residents, MiCA does not apply. However, this is difficult to enforce perfectly and is not a viable long-term strategy if the EU market is important to you. The only compliant way to access the EU market is to establish an EU subsidiary and obtain a CASP license.

Q5: What are the penalties for non-compliance with DORA or MiCA?

A: The penalties are severe. For MiCA, they can include large fines and cease-and-desist orders. For DORA, fines can reach up to €5 million or 10% of annual turnover, along with potential license suspension and personal bans for management. The reputational damage from a public enforcement action can be just as costly.

Q6: How does the AML "Travel Rule" fit in with MiCA and DORA?

A: The Travel Rule, which requires the sharing of sender and receiver information for crypto transfers, is part of a separate but parallel EU regulation—the Transfer of Funds Regulation (TFR). It came into force alongside MiCA. If you are a CASP under MiCA, you must also comply with the TFR. This is not just another item on a checklist; a robust, working solution for TFR compliance is a baseline operational capability and a critical, upfront hurdle for any firm seeking MiCA authorization.



Simplify Your Full Compliance with Hacken

See Hacken's solutions for every key requirement

The 4-Step CASP/VASP Compliance Journey

1 Readiness Assessment & Strategic Roadmap

What we do: We conduct in-depth interviews with your key stakeholders, gather existing evidence, and perform a gap analysis against every relevant framework.

Your outcome: You receive a clear Compliance Posture Report and a strategic 12-month security roadmap with defined budget considerations and achievable milestones.

2 Technical Testing & Risk Identification

What we do: Our elite teams execute comprehensive TLPT, web, API & mobile penetration tests, L1/L2 Blockchain and smart contract audits, plus cloud/Infrastructure-as-Code (IaC) security reviews.

Your outcome: You get a detailed, risk-ranked findings dossier and a clear, prioritized remediation guide – so you know exactly what to fix and in what order.

3 Guided Remediation & Implementation

What we do: We don't just point out problems; we help you solve them. We assist in drafting policies, rolling out processes, integrating essential tools (from Web2 monitoring to our proprietary Hacken Extractor for blockchain intelligence), and retesting until every vulnerability is demonstrably closed.

Your outcome: A fully operational Information Security Management System (ISMS) and a verified-closure letter ready for inspector review, proving your commitment and diligence.

4 Certification & Licensing Support

What we do: We meticulously package all evidence, expertly manage every interaction with regulators or certification bodies, and tackle any last-minute queries in real time.

Your outcome: Your licence or certificate is officially issued. Our engagement only concludes when "approved" is the official word. No exceptions.

Why Teams Choose CASP/VASP Compliance

Unified compliance roadmap

We distill MiCA, DORA, VARA, ISO 27001, CCSS, CIS Controls (and more) into one clear, actionable master plan tailored to your business.

Your dedicated compliance strike team

One cohesive unit – ISO auditors, Web2/Web3 pentesters, DeFi researchers, DevSecOps engineers – operating from a single playbook for you.

Guaranteed regulator liaison & support

We don’t just prepare paperwork. We build your evidence pack, join every regulator call, and manage the process until you're approved.

Executive clarity & confidence

Real-time dashboards, KPI trackers, and signed attestation letters provide the transparent oversight and assurance your stakeholders demand.

Predictable progress, controlled budget

Our sprint-based delivery, fixed milestones, and transparent pricing ensure compliance accelerates, not hinders, your time-to-market.

Hacken is here to be your partner on this journey.

Whether you need a DORA readiness assessment, a security audit to meet MiCA's liability standards, or guidance on your license application, our team has the expertise to bolster your compliance and security efforts.

Let’s Build Your Compliance Together →

About Hacken

Hacken is an end-to-end blockchain security & compliance partner for digital assets.

Unlike traditional providers, Hacken was born on blockchain—combining deep Web3 expertise with enterprise-grade quality, AI-powered offensive security, and globally recognized certifications. Since 2017, Hacken has been trusted by 1,500 adopters including the European Commission, ADGM, MetaMask, Ethereum Foundation, and Binance to secure the new digital frontier.

We bring top-tier, blockchain-native expertise and proven credibility to help organizations secure their infrastructure and meet modern digital asset regulations with confidence.

Chat with our experts now →



Bryn Bennett
Partner, Security & Compliance

LinkedIn

Telegram

8+
Years of expertise

130+
Team members

180+
Partners

1,500+
Clients

$180B+
Secured

Follow us on

linkedin.com/hacken

x.com/hackenclub

Contact us today

hacken.io/contact