TITLE V: AUTHORISATION AND OPERATING CONDITIONS FOR CRYPTO-ASSET SERVICE PROVIDERS (CASPs) – [A(26): 59-85]

Chapter 1: Authorization of CASPs

Article 59: Authorization of Crypto-Asset Service Providers (CASPs)

Article 59 of **Regulation (EU) 2023/1114 (MiCA)** establishes the **mandatory authorization framework** for all entities providing **crypto-asset services** in the EU.

1. Authorization Requirement (Paragraph 1)

Who Needs Authorization?

- **(1a)** Any **legal person or undertaking** (company, LLC, etc.) providing crypto services **must obtain authorization** under Article 63.
- **(1b) Exemptions**: The following **already-regulated financial entities** can offer crypto services **without separate MiCA authorization** (under Article 60):
    - Credit institutions (banks)
    - Investment firms (MiFID II-regulated)
    - Electronic money institutions (EMIs)
    - UCITS/AIFM fund managers
    - Market operators & central securities depositories (CSDs)

Why?
Prevents unregulated entities from offering risky crypto services while allowing traditional finance firms to expand into crypto under existing licenses.

2. Registered Office & Management (Paragraph 2)

Authorized CASPs must:
☑ **Have a registered office in an EU Member State** (where they operate).
☑ **Effective management in the EU** (key decisions made within the EU).
☑ **At least one resident director** in the EU.

Purpose: Ensures CASPs are **sufficiently established** in the EU for supervision.

3. Non-Legal Entities (Paragraph 3)

- Some entities (e.g., partnerships, trusts) **without legal personality** can still obtain authorization **if**:
    - Their legal structure **protects third-party interests** like a legal entity.
    - They are subject to **equivalent prudential supervision**.

Example: A German GmbH & Co. KG (partnership with limited liability) could qualify.

4. Ongoing Compliance (Paragraph 4)

- CASPs must **continuously** meet authorization conditions (e.g., capital, governance, client safeguards).
- **Failure → License revocation** (Article 64).

5. Misleading Practices Ban (Paragraph 5)

- **No unauthorized entity** may:
    - Use names like "crypto exchange" or "digital asset custodian."
    - Issue marketing suggesting they are regulated.
- **Goal**: Prevents scams like fake "licensed" crypto platforms.

6. Scope of Authorization (Paragraph 6)

- NCAs must **specify which services** a CASP is authorized for, e.g.:
    - "Authorized for custody & trading, but not portfolio management."
- **Why?** Ensures clarity on permitted activities.

7. EU Passporting Rights (Paragraph 7)

- Once authorized, a CASP can:
    - Operate **EU-wide via branches** or **cross-border without physical presence**.
    - No need for **additional licenses** in other Member States.
- **Exception**: Must **notify** host NCAs before expanding (Article 65).

Example: A French CASP can serve German clients without a German license.

8. Extending Authorization (Paragraph 8)

- To **add new services** (e.g., custody → trading), CASPs must:
    1. **Submit updated documentation** (per Article 62).
    2. Undergo a new **NCA review** (same 3-month timeline as Article 63).

Key Implications of Article 59:

Aspect	Requirement
Who needs a license?	All crypto service providers except exempt traditional finance firms (Art. 60).
Where to apply?	NCA of the **home Member State** (e.g., BaFin for Germany, AMF for France).
Passporting	Single license = EU-wide operation (no extra approvals).
Ongoing rules	Must **always** meet capital, governance, and consumer protection standards.
Penalties	Unauthorized providers face **fines, bans, or criminal charges**.

Article 60: Provision of Crypto-Asset Services by Certain Financial Entities

Article 60 of **Regulation (EU) 2023/1114 (MiCA)** establishes a **simplified notification regime** for **traditional financial institutions** that wish to provide crypto-asset services **without requiring separate MiCA authorization**. Below is a detailed breakdown of each provision.

1. Overview of Article 60

- **Purpose**: Allows **already-regulated financial entities** (e.g., banks, investment firms, e-money institutions) to offer crypto services **without a separate MiCA license**, provided they **notify their regulator** in advance.
- **Key Benefit**: Avoids **duplicate licensing** for firms already supervised under EU financial laws (e.g., MiFID II, CRD, EMD).
- **Who Qualifies?**
    - Credit institutions (banks)
    - Central securities depositories (CSDs)
    - Investment firms
    - Electronic money institutions (EMIs)
    - UCITS/AIFM fund managers
    - Market operators

2. Key Provisions & Requirements

(1) Credit Institutions (Banks) – Paragraph 1

- **Can provide any crypto-asset service** (e.g., custody, trading, advice).
- **Must notify home NCA** (e.g., ECB, BaFin, ACPR) **40 working days before starting services**.
- **No MiCA authorization needed** (since banks are already heavily regulated).

(2) Central Securities Depositories (CSDs) – Paragraph 2

- **Only allowed to provide custody & administration of crypto-assets** (not trading/exchange).
- **Must notify home NCA 40 days in advance**.
- **Deemed equivalent to securities account services** under **Regulation (EU) No 909/2014 (CSDR)**.

(3) Investment Firms – Paragraph 3

- **Can provide crypto services equivalent to their MiFID II permissions**:

Crypto Service	**Equivalent MiFID II Activity**
Custody	Ancillary service (Sec B, Pt 1, Annex I)
Trading Platform	MTF/OTF operation (Sec A, Pt 8-9)
Exchange (crypto ↔ fiat)	Dealing on own account (Sec A, Pt 3)
Execution of orders	Execution for clients (Sec A, Pt 2)
Placing crypto-assets	Underwriting/placing (Sec A, Pt 6-7)
Advice on crypto	Investment advice (Sec A, Pt 5)
Portfolio management	Portfolio management (Sec A, Pt 4)

- **Must notify home NCA 40 days before launch**.

(4) Electronic Money Institutions (EMIs) – Paragraph 4

- **Only allowed to provide**:
    - Custody of **their own e-money tokens** (not third-party tokens).
    - Transfer services for **their own e-money tokens**.
- **Must notify home NCA 40 days in advance**.

(5) UCITS & AIFMs (Fund Managers) – Paragraph 5

- **Can provide crypto services equivalent to their existing permissions**:
    - Reception/transmission of orders (similar to financial instruments).
    - Advice on crypto (equivalent to investment advice).
    - Portfolio management (crypto assets).
- **Must notify home NCA 40 days before launch**.

(6) Market Operators – Paragraph 6

- **Can operate crypto trading platforms** (equivalent to MiFID MTFs/OTFs).
- **Must notify home NCA 40 days before launch**.

3. Notification Requirements (Paragraph 7)

Entities must submit the following **detailed documentation** to their NCA:
✓ **Program of operations** (services offered, marketing plans).
✓ **AML/CFT controls** (risk assessment, internal policies).
✓ **IT security & business continuity plans**.
✓ **Client asset segregation procedures**.
✓ **Trading platform rules** (if applicable).
✓ **Pricing methodology** (for exchange services).
✓ **Staff qualifications** (for advice/portfolio management).

NCA Review:

- NCAs have **20 working days** to confirm the notification is complete.
- If incomplete, the firm has **20 more days** to submit missing info.
- **Services cannot start until notification is complete**.

4. Exemptions & Special Rules

(9) No Duplicate Submissions

- Firms **don't need to resubmit** previously filed documents (if still valid).

(10) Exemption from MiCA Authorization Rules

- These entities **do not need to comply with**:
    - Full MiCA application (Art. 62).
    - MiCA capital requirements (Art. 67).
    - MiCA acquisition rules (Arts. 83-84).

(11) Revocation of Rights

- If the firm **loses its primary license** (e.g., a bank loses its banking license), its right to offer crypto services is **automatically revoked**.

5. ESMA's Role (Paragraphs 12-14)

- **NCAs must share notifications with ESMA**, which maintains a **public register** of crypto service providers.
- **ESMA & EBA** will develop **technical standards** (by June 2024) to harmonize:
    - **Notification formats** (implementing standards).

- **Detailed content requirements** (regulatory standards).

6. Key Takeaways

☑ **Simplified Entry for Traditional Finance**: Banks, investment firms, and EMIs can expand into crypto **without a new license**.
☑ **40-Day Notification Rule**: Must inform regulators before launching services.
☑ **Limited Scope for Some Firms**:

- **CSDs** → Only custody.
- **EMIs** → Only their own e-money tokens.
  ☑ **No Passporting Needed**: Firms can operate EU-wide under existing financial licenses.
  ☑ **Strict AML/IT Requirements**: Must prove compliance with anti-fraud and cybersecurity rules.

Article 61: Provision of Crypto-Asset Services at the Client's Exclusive Initiative

Article 61 of **Regulation (EU) 2023/1114 (MiCA)** creates a **limited exemption** for **third-country (non-EU) crypto firms** that provide services **solely at the request of EU-based clients**, without actively marketing in the EU. Below is a detailed breakdown.

1. Core Rule: The "Reverse Solicitation" Exemption (Paragraph 1)

When Does It Apply?

A **third-country (non-EU) crypto firm** does **not need MiCA authorization** if:

- An **EU client** (individual or business) **initiates contact on its own exclusive initiative** to request a crypto service.
- The firm **does not solicit** EU clients (no advertising, promotions, or direct outreach).

Key Conditions

✓ **Strictly client-initiated**: The EU client must reach out **without any prior inducement** (e.g., cold calls, ads, referrals).
✓ **No circumvention**: If the firm (or its affiliates) markets services in the EU, the exemption **does not apply**.
✓ **Contract disclaimers ignored**: A clause claiming "client-initiated" is **not valid** if there was prior solicitation.

Example:

- ☑ **Allowed**: A German investor finds a Swiss crypto exchange online and contacts them directly to trade.
- ❌ **Not Allowed**: The Swiss exchange runs Google ads targeting EU users or hires EU-based promoters.

2. Limits of the Exemption (Paragraph 2)

Even if the service is client-initiated:

- The **third-country firm cannot "upsell" new services or assets** to the client.
- The exemption **only covers the specific service requested initially**.

Example:

- If the client first requested **trading**, the firm cannot later offer **custody or lending** without MiCA authorization.

3. ESMA's Role: Anti-Circumvention Rules (Paragraph 3)

To prevent abuse, **ESMA will issue guidelines by December 2024** clarifying:

- **What counts as "solicitation"**:
  - Ads, partnerships with EU firms, social media targeting, affiliate schemes.
- **Supervisory practices to detect evasion**:
  - How regulators should investigate firms **pretending** to rely on reverse solicitation.

Goal: Stop offshore firms from **de facto operating in the EU** without complying with MiCA.

4. Why This Matters

For Third-Country Firms

- **No EU license needed** if services are **truly passive** (but risky if regulators disagree).
- **Cannot systematically target EU clients** without authorization.

For EU Clients

- Still able to access global crypto services **if they seek them out**.
- **No MiCA protections** (e.g., fund segregation, dispute resolution) for these transactions.

For Regulators

- Prevents **regulatory arbitrage** (offshore firms avoiding EU rules).
- ESMA guidelines will **tighten enforcement** against fake "client-initiated" schemes.

5. Key Takeaways

Aspect	**Rule**
Exemption applies	Only if EU client contacts firm **without any prior solicitation**.
Marketing bans	No ads, referrals, or promotions in the EU.
Service limits	Only covers the **initial service requested** (no upselling).
ESMA oversight	Strict guidelines by 2024 to prevent abuse.
Risks for firms	If wrongly claimed, penalties include **fines or EU operation bans**.

Practical Implications

- **For Crypto Exchanges (e.g., Binance, Kraken)**:
  - Must **block EU IPs** or get MiCA authorization unless **100% passive**.
- **For EU Institutional Investors**:
  - Can still use offshore services **if they initiate contact**.
- **For Regulators**:
  - Will monitor **shadow marketing** (e.g., via influencers, "unofficial" referrals).

Article 62: Application for Authorization as a Crypto-Asset Service Provider (CASP)

Article 62 of **Regulation (EU) 2023/1114 (MiCA)** establishes the **mandatory application process** for any entity seeking to become a **licensed crypto-asset service provider (CASP)** in the EU. Below is a structured breakdown of its key provisions.

1. Who Must Apply? (Paragraph 1)

- **Legal persons or undertakings** (companies, LLCs, etc.) that intend to provide **any crypto-asset service** in the EU.
- **Exception**: Firms already authorized under **MiFID II, EMD, or other EU financial laws** (see **Article 60**) do not need separate MiCA authorization.

Application Submission:

- Must be filed with the **National Competent Authority (NCA)** of the **home Member State** (e.g., BaFin for Germany, AMF for France).

2. Required Application Documents (Paragraph 2)

The application must include **detailed information** across **six key areas**:

(A) Entity Identification & Structure

- Legal name, trade names, LEI (Legal Entity Identifier), website, contact details.
- Legal form (e.g., GmbH, SAS, Ltd.).
- Articles of association (if applicable).

(B) Business Operations

- **Program of operations**:
  - Types of crypto services to offer (e.g., custody, trading, advice).
  - Marketing strategy (geographic focus, target clients).
- **Prudential safeguards**: Proof of compliance with **capital requirements** (Article 67).

(C) Governance & Fit-and-Proper Checks

- **Management board**:
  - Proof of **good repute** (no criminal/regulatory penalties).
  - **Expertise** in crypto/financial services.
- **Shareholders with >10% stakes ("qualifying holdings")**:
  - Must also pass **reputation checks**.

(D) Risk Management & Compliance

- **Internal controls**:
  - AML/CFT (anti-money laundering) policies.
  - Business continuity plans (e.g., for cyberattacks).
- **IT security**:
  - Technical documentation of systems (e.g., cold/hot wallet setup).

- Non-technical summary for regulators.

(E) Client Asset Protection

- **Segregation of funds**: How client crypto/fiat will be separated from company assets.
- **Complaints handling**: Procedures for resolving client disputes.

(F) Service-Specific Disclosures

Service	Required Documentation
Custody	Custody policy (e.g., cold storage procedures).
Trading Platform	Market abuse detection systems.
Exchange Services	Pricing methodology (must be fair/non-discriminatory).
Order Execution	Execution policy (best practices).
Advice/Portfolio Mgmt.	Proof of staff qualifications.
Transfer Services	Description of transfer mechanisms.

3. Fit-and-Proper Checks (Paragraph 3)

Applicants must prove:
☑ **No criminal records** for management/shareholders (fraud, AML violations, etc.).
☑ **Relevant expertise** (e.g., crypto, finance, IT security).
☑ **Time commitment** (directors must dedicate sufficient attention).

4. Avoidance of Duplicate Submissions (Paragraph 4)

- If the applicant **already submitted** equivalent documents under **other EU laws** (e.g., MiFID II, EMD), they **do not need to resubmit** unless outdated.
- **Example**: A German e-money institution applying for crypto custody can reuse its BaFin filings.

5. ESMA's Role: Standardizing Applications (Paragraphs 5-6)

- **By June 2024**, ESMA and EBA will develop:
  - **Regulatory Technical Standards (RTS)**:
    - Further details on required documents (e.g., IT security depth).
  - **Implementing Technical Standards (ITS)**:
    - Standardized **application forms/templates**.
- **Goal**: Ensure **uniformity** across EU NCAs.

6. Key Takeaways

Step	Requirement
Who Applies?	Any firm offering crypto services in the EU (except exempt traditional finance entities).
Where to Apply?	NCA of the **home Member State** (e.g., ACPR for France).
Timeline	NCAs must decide within **3 months** (Article 63).

Step	Requirement
Critical Docs	Business plan, governance proof, AML controls, IT security, client safeguards.
Post-Authorization	Must **continuously comply** (e.g., capital, reporting).

Article 63: Assessment of Authorization Applications for Crypto-Asset Service Providers (CASPs)

Article 63 of **Regulation (EU) 2023/1114 (MiCA)** details how **National Competent Authorities (NCAs)** evaluate and decide on applications for **CASP licenses**. Below is a structured breakdown of the process, timelines, and key requirements.

1. Application Submission & Initial Review (Paragraphs 1-4)

Key Steps

- **Acknowledgment of Receipt**
  - NCAs must **confirm receipt** of the application **within 5 working days**.
- **Completeness Check**
  - Within **25 working days**, NCAs verify if **all documents** (per Article 62) are submitted.
  - If incomplete, NCAs set a **deadline** for missing info (no specified duration, but typically short).
  - **Risk**: Applications may be **rejected if incomplete** after the deadline.
- **Notification of Completeness**
  - Once complete, NCAs **notify the applicant** and begin the **substantive assessment**.

2. Substantive Assessment (Paragraphs 5-9)

(A) Consultation with Other Authorities (Paragraph 5)

- NCAs **must consult** other EU regulators if the applicant is:
  - A **subsidiary** of a bank, investment firm, e-money institution, etc.
  - **Controlled by the same entity** as a regulated financial firm.
- **Purpose**: Avoid regulatory gaps in group-wide supervision.

(B) AML/CFT Checks (Paragraph 6)

NCAs must:

1. **Consult financial intelligence units** to confirm no ongoing **money laundering/terrorist financing (ML/TF)** investigations.
2. **Verify compliance** with AML rules for high-risk third countries (if applicable).
3. Ensure **appropriate procedures** for **beneficial ownership transparency**.

(C) "Close Links" Review (Paragraphs 7-8)

- Authorization can be **denied** if:
  - The applicant's **ties to other entities** (e.g., parent companies, shareholders) **hinder effective supervision**.
  - Third-country laws **prevent proper oversight** (e.g., secrecy jurisdictions).

(D) Final Decision Timeline (Paragraph 9)

- NCAs have **40 working days** (after deeming the application complete) to:
  - Assess compliance with **MiCA Title V** (CASP rules).
  - Issue a **fully reasoned decision** (approval or rejection).
- **Complexity factor**: Assessment considers the **scale/risk** of services (e.g., custody vs. trading).

3. Grounds for Refusal (Paragraph 10)

NCAs **must reject** applications if:
❌ **Management body** is unfit (e.g., lacks expertise, poses ML/TF risks).
❌ **Shareholders with >10% stakes** fail **good repute checks**.
❌ **Non-compliance** with MiCA rules (e.g., insufficient capital, weak governance).

4. ESMA & EBA Guidelines (Paragraph 11)

- By **June 2024**, ESMA/EBA will issue **joint guidelines** on:
  - Assessing **management/shareholder suitability**.
  - Defining **"good repute"** standards.
- **Goal**: Harmonize approval criteria across the EU.

5. Requests for Additional Information (Paragraph 12)

- NCAs may request **extra documents** (by **Day 20** of the 40-day assessment).
- The **clock stops** until the applicant responds (max **20 working days**).
- **No further suspensions** allowed for follow-up queries.

6. Post-Decision Steps (Paragraph 13)

- **Approved CASPs**: NCAs notify **ESMA within 2 days** for inclusion in the **EU-wide crypto register**.
- **Rejections**: Also reported to ESMA.

7. Key Takeaways

Stage	Timeline	Key Requirements
Submission	Day 0	Full application per **Article 62**.
Acknowledgment	Within 5 days	NCAs confirm receipt.
Completeness Check	Within 25 days	NCAs verify documents; request missing info if needed.
Substantive Review	40 days (total)	AML checks, "close links" review, compliance with MiCA.
Final Decision	Day 65-70*	Approval/rejection with detailed reasoning.

**Assuming no suspension for missing info.*

Why This Matters

- **Investor Protection**: Ensures only **qualified, compliant firms** operate.
- **Regulatory Efficiency**: Clear **40-day timeline** (vs. indefinite waits in some jurisdictions).
- **EU-Wide Consistency**: ESMA/EBA guidelines prevent **divergent national standards**.

Article 63 creates a **transparent, rigorous licensing process** for crypto firms, balancing **market access** with **financial stability**. Its success depends on **NCAs' capacity** and **ESMA's 2024 guidelines**.

Article 64: Withdrawal of Authorization for Crypto-Asset Service Providers (CASPs)

Article 64 of **Regulation (EU) 2023/1114 (MiCA)** defines the **circumstances and procedures** under which a CASP's authorization can be **withdrawn (revoked)** by regulators. This ensures only compliant and operational firms continue to provide crypto services in the EU.

1. Mandatory Withdrawal (Paragraph 1)

Competent authorities **must revoke** a CASP's license if it:

Grounds for Withdrawal	Explanation
(a) Non-use of license	Fails to start operations **within 12 months** of authorization.
(b) Voluntary renunciation	Explicitly gives up its license (e.g., exits the market).
(c) Inactivity	Does not provide services for **9 consecutive months**.
(d) Fraudulent authorization	Obtained license via **false statements** in the application.
(e) Non-compliance	No longer meets MiCA requirements (e.g., capital, governance) and **fails to fix issues** within a set deadline.
(f) AML/CFT failures	Lacks effective **anti-money laundering (AML)** or **counter-terrorist financing (CFT)** systems.
(g) Serious MiCA breaches	Violates key rules (e.g., client asset protection, market integrity).

Example:

- A CASP stops offering services for **10 months** → **License revoked**.
- A CASP **lied about its management's criminal record** → **License revoked for fraud**.

2. Discretionary Withdrawal (Paragraph 2)

NCAs **may revoke** a license if:

- The CASP breaches **AML/CFT laws** (Directive (EU) 2015/849).
- It **loses its payment/e-money license** and doesn't fix the issue within **40 days**.

Example:

- A CASP also operating as an **e-money institution** loses its EMI license → NCA **may** revoke its MiCA license.

3. Notification & EU-Wide Effects (Paragraph 3)

- NCAs must **immediately notify**:
  - **ESMA** (for the EU crypto register).
  - **Host Member States** (if the CASP operated cross-border).
- **Result**: The CASP **cannot operate anywhere in the EU** after withdrawal.

4. Partial Withdrawal (Paragraph 4)

- NCAs can **limit revocation to specific services** (e.g., ban custody but allow trading).
- **Example**: A CASP fails **custody safeguards** but maintains proper trading systems → Only **custody authorization** is withdrawn.

5. Consultation with Other Authorities (Paragraphs 5-6)

Before revoking, NCAs must:

- **Consult other EU regulators** if the CASP is part of a **group** (e.g., subsidiary of a bank).
- **Optionally consult AML supervisors** if the withdrawal relates to **money laundering risks**.

Goal: Ensure coordinated supervision.

6. Requests for Reassessment (Paragraph 7)

- **EBA, ESMA, or host NCAs** can request a **review** if they suspect a CASP no longer complies with MiCA.
- **Example**: ESMA flags a CASP for **market manipulation** → Requests home NCA to reassess its license.

7. Client Asset Protection (Paragraph 8)

- CASPs must have **wind-down plans** to **safely transfer client crypto/funds** to another provider if their license is withdrawn.
- **Purpose**: Prevents **loss or freezing of assets** (e.g., avoids situations like FTX).

8. Key Takeaways

Aspect	**Rule**
Automatic revocation	If inactive, non-compliant, or fraudulent.
Partial withdrawal	Possible (e.g., only ban custody services).
EU-wide effect	Withdrawn CASPs cannot operate anywhere in the EU.
Client protection	Must ensure orderly transfer of assets.

Article 65: Cross-Border Provision of Crypto-Asset Services

Article 65 of **Regulation (EU) 2023/1114 (MiCA)** establishes the framework for **Crypto-Asset Service Providers (CASPs)** to operate across the EU using a **"passporting" system**, similar to traditional financial services. Below is a detailed breakdown of its provisions.

1. Overview of Article 65

- **Purpose**: Allows a CASP authorized in one EU Member State (**home state**) to provide services in **other Member States (host states)** without needing additional licenses.
- **Key Benefit**: Eliminates **duplicate regulatory approvals**, enabling seamless EU-wide expansion.

2. Key Provisions & Process

(1) Notification Requirement (Paragraph 1)

Before operating cross-border, the CASP must submit the following to its **home NCA**:
✓ **List of target Member States** where services will be offered.
✓ **Types of crypto services** to be provided (e.g., custody, trading).

✓ **Planned start date** for cross-border operations.
✓ **Other non-MiCA activities** (e.g., traditional payment services).

Example:
A German CASP (authorized by BaFin) wants to serve clients in France and Italy → Submits this info to BaFin.

(2) NCA Communication (Paragraphs 2-3)

- The **home NCA** (e.g., BaFin) must **forward this info** within **10 working days** to:
  - **Host NCAs** (e.g., AMF for France, CONSOB for Italy).
  - **ESMA & EBA** (for EU-wide oversight).
- The home NCA then **notifies the CASP** that the passporting process has been initiated.

(3) Timeline for Launch (Paragraph 4)

The CASP can start cross-border services:
☑ **Immediately** after receiving confirmation from its home NCA.
☑ **No later than 15 calendar days** after submission (if no response).

No approval needed: Host NCAs **cannot block** the CASP's entry but can supervise compliance.

3. Key Takeaways

Step	Responsibility	Timeline
CASPs notify home NCA	Submit target markets/services.	Before expansion.
Home NCA shares info	Send to host NCAs, ESMA, EBA.	Within 10 working days.
CASP can launch	Start operations in host states.	Immediately or max 15 days after submission.

Chapter 2: Obligation for all the CASPs

Article 66: Obligation to act honestly, fairly and professionally

Article 66 of Regulation (EU) 2023/1114 (MiCA) establishes stringent requirements for **crypto-asset service providers (CASPs)** to ensure transparency, client protection, and environmental accountability.

1. Core Obligations for CASPs

a. Duty of Conduct (Paragraph 1)

- CASPs must act **honestly, fairly, and professionally**, prioritizing the **best interests of clients** (including prospective clients).
- **Example**: A crypto exchange must avoid conflicts of interest, such as prioritizing proprietary trades over client orders.

b. Transparency in Communications (Paragraph 2)

- All information provided to clients must be **fair, clear, and non-misleading**.
- **Marketing materials** (e.g., ads, social media posts) must be explicitly labeled as such.
- **Prohibition**: Misleading claims about crypto-asset benefits, whether intentional or negligent.
    - *Example*: A platform cannot falsely advertise a token as "risk-free" or guarantee returns.

c. Risk Warnings (Paragraph 3)

- CASPs must **warn clients of risks** associated with crypto transactions.
- For specific services (trading platforms, exchanges, advice, portfolio management), CASPs must provide **hyperlinks to crypto-asset white papers**.
    - *Purpose*: Ensure clients can access detailed information (e.g., project goals, risks, technical specs).

d. Fee Transparency (Paragraph 4)

- **Pricing, costs, and fees** must be publicly disclosed in a **prominent website section**.
    - *Example*: A crypto brokerage must clearly list trading fees, withdrawal charges, and spreads.

e. Environmental Disclosures (Paragraph 5)

- CASPs must publish **environmental impact information** for crypto-assets they service, focusing on:
    - **Consensus mechanisms** (e.g., Proof-of-Work, Proof-of-Stake).
    - **Adverse impacts**: Energy use, greenhouse gas emissions, waste, and natural resource consumption.
    - *Source*: Data may be drawn from crypto-asset white papers.
    - *Example*: A Bitcoin exchange must disclose Bitcoin’s high energy consumption due to Proof-of-Work.

2. Regulatory Technical Standards (Paragraph 6)

- **ESMA and EBA** will develop **technical standards** by **30 June 2024** to standardize:

    - **Content**: Specific environmental metrics (e.g., CO2 emissions per transaction).
    - **Methodologies**: How to calculate and verify environmental impacts.
    - **Presentation**: Format for disclosing sustainability indicators (e.g., dashboards, labels).
- **Updates**: Standards must evolve with technological advancements (e.g., shifts to renewable energy in mining).

3. Key Implications

Requirement	Practical Impact
Client-Centric Conduct	CASPs must avoid conflicts of interest and prioritize client welfare.
Risk Communication	Clients receive clear warnings and access to white papers for informed decisions.
Fee Transparency	No hidden charges; fosters trust and comparability between platforms.
Environmental Accountability	Drives adoption of eco-friendly consensus mechanisms (e.g., Proof-of-Stake).

Article 67: Prudential Requirements for Crypto-Asset Service Providers

Article 67 of the **Markets in Crypto-Assets Regulation (MiCAR)** establishes **prudential safeguards** that **Crypto-Asset Service Providers (CASPs)** must maintain to ensure financial stability, operational resilience, and consumer protection.

Key Provisions of Article 67

1. Minimum Prudential Safeguards (Paragraph 1)

CASPs must maintain **prudential safeguards** equal to the **higher** of:

- **(a) Permanent minimum capital** (as per **Annex IV**, based on the type of crypto-asset services provided).
- **(b) 25% of the previous year's fixed overheads** (reviewed annually).

Example:

- If a CASP's **minimum capital requirement** (Annex IV) is **€50,000**, but **25% of last year's fixed overheads** is **€100,000**, the CASP must hold **€100,000** in prudential safeguards.

2. New CASPs (Paragraph 2)

- If a CASP has **not been in business for a full year**, it must use **projected fixed overheads** (from its **first 12-month business plan**) for the calculation.

3. Calculation of Fixed Overheads (Paragraph 3)

Fixed overheads are derived from the **most recent audited financial statements** (or supervisor-validated statements if unaudited). The following **deductions** apply:

- **(a) Profit-dependent staff bonuses**
- **(b) Profit-sharing for employees/directors**

- **(c) Discretionary profit appropriations**
- **(d) Non-recurring expenses**

This ensures only **essential fixed costs** (e.g., rent, salaries, IT infrastructure) are considered.

4. Forms of Prudential Safeguards (Paragraph 4)

CASPs can meet prudential requirements through:

- **(a) Own funds** (Common Equity Tier 1 capital, per **Regulation (EU) No 575/2013** – the **Capital Requirements Regulation - CRR**).
- **(b) An insurance policy or comparable guarantee** (covering all EU jurisdictions where services are offered).

5. Insurance Policy Requirements (Paragraph 5 & 6)

If using an **insurance policy**, it must:

- Be **publicly disclosed** on the CASP's website.
- Have a **minimum 1-year term** with **90-day cancellation notice**.
- Be issued by an **authorized EU/national insurer**.
- Cover risks including:
    - **Loss of documents**
    - **Misrepresentation/misleading statements**
    - **Breaches of legal obligations** (e.g., confidentiality, conflicts of interest)
    - **Business disruptions/system failures**
    - **Negligence in safeguarding client assets**
    - **Liability under MiCAR Article 75(8)** (e.g., compensation for losses due to non-compliance).

Article 68: Governance Arrangements

Article 68 of the **Markets in Crypto-Assets Regulation (MiCAR)** establishes **governance and operational requirements** for **Crypto-Asset Service Providers (CASPs)** to ensure **integrity, competence, risk management, and business continuity**.

Key Provisions of Article 68

1. Management Body Requirements (Paragraph 1 & 2)

- **Good Repute & Expertise:**
    - Members of the **management body** (e.g., directors, executives) must have **good repute, appropriate knowledge, skills, and experience**.
    - They **must not** have been convicted of **money laundering (ML), terrorist financing (TF), or other serious offenses**.
    - They must **commit sufficient time** to their duties.

- **Shareholders & Qualifying Holders:**
    - **Major shareholders** (direct/indirect) must also be of **good repute** and free from ML/TF convictions.

Why?
Prevents criminals from controlling CASPs and ensures competent leadership.

2. Measures Against Harmful Influence (Paragraph 3)

- If a **shareholder's influence** risks **unsound management**, regulators can:
    - **Impose penalties** on management.
    - **Suspend voting rights** of problematic shareholders.
    - Seek **judicial intervention**.

Why?
Prevents **undue influence** that could harm the CASP's stability or compliance.

3. Compliance Policies & Procedures (Paragraph 4-6)

- CASPs must implement **effective policies** to comply with MiCAR.
- **Hire skilled personnel** matching the **scale and complexity** of services.
- **Management must regularly review** compliance effectiveness (e.g., risk controls, AML checks).

Why?
Ensures **operational integrity** and **regulatory adherence**.

4. Business Continuity & ICT Security (Paragraph 7)

- CASPs must ensure **uninterrupted service** via:
    - **Resilient IT systems** (per **Regulation (EU) 2022/2554** – DORA).
    - **Business continuity plans** (including **ICT recovery plans**).
    - **Data preservation & quick recovery** in case of disruptions.

Why?
Prevents **service failures** (e.g., hacks, outages) that could harm clients.

5. Risk Management & Record-Keeping (Paragraph 8-9)

- **Risk Assessment & AML Compliance:**
    - Must follow **Directive (EU) 2015/849** (AMLD5).
    - Regularly **monitor and update** risk controls.
- **Record-Keeping:**
    - **Keep detailed logs** of all **transactions, orders, and activities** for **5 years** (extendable to **7 years** if requested by regulators).
    - Records must be **accessible to authorities** and **clients upon request**.

Why?

- Helps **regulators supervise** CASPs.

- Ensures **transparency** and **accountability**.

6. ESMA's Role (Paragraph 10)

- **ESMA** will develop **Regulatory Technical Standards (RTS)** to specify:
  - **Business continuity measures** (Paragraph 7).
  - **Record-keeping details** (Paragraph 9).
- Deadline: **30 June 2024** (submission to the EU Commission).

Why?
Ensures **uniform implementation** across the EU.

Article 69: Information to Competent Authority

Article 69 of MiCAR (Notification of Changes to Management Body)

Article 69 of the **Markets in Crypto-Assets Regulation (MiCAR)** imposes a **transparency obligation** on **Crypto-Asset Service Providers (CASPs)** regarding changes in their **management body** (e.g., board members, executives).

Key Requirements of Article 69

1. Mandatory Notification to Competent Authority

- CASPs must **immediately notify** their national regulator (**competent authority**) of **any changes** in their **management body**.
- The notification must be made **before** the new member starts their role.

2. Information to Be Provided

- The CASP must submit **all necessary details** to allow the regulator to **assess compliance with Article 68** (governance requirements).
  - This includes **proof of good repute, qualifications, and experience** of the new member.
  - Regulators may check for **past criminal convictions** (e.g., money laundering, frauds.

Article 70: Safekeeping of Clients' Crypto-Assets and funds

Article 70 of the **Markets in Crypto-Assets Regulation (MiCAR)** establishes **strict safeguarding rules** to protect **clients' crypto-assets and funds** held by **Crypto-Asset Service Providers (CASPs)**. It ensures **asset segregation, insolvency protection, and prevention of misuse** by service providers.

Key Provisions of Article 70

1. Safeguarding Clients' Crypto-Assets (Paragraph 1)

- **CASPs holding clients' crypto-assets** (or **access keys**) must:

    - **Protect ownership rights** (especially in case of **insolvency**).
    - **Prevent misuse** (e.g., using clients' crypto-assets for their own trading).
- **Mechanisms may include:**
    - **Cold storage solutions** (offline wallets).
    - **Multi-signature controls**.
    - **Third-party custodians**.

Why?
Prevents **loss, theft, or unauthorized use** of clients' crypto holdings.

2. Safeguarding Clients' Fiat Funds (Paragraph 2 & 3)

- **If CASPs hold clients' cash (non-e-money tokens):**
    - Must **protect ownership rights** and **prevent commingling** (mixing with the CASP's own funds).
    - **By the next business day**, must deposit funds in:
        - A **credit institution (bank)** or **central bank**.
        - In a **separate, identifiable account** (not mixed with the CASP's funds).

Why?
Ensures **client money is safe** even if the CASP goes bankrupt.

3. Payment Services (Paragraph 4)

- **CASPs can offer payment services** (e.g., fiat-to-crypto transactions) **only if:**
    - They (or a third party) are **authorized under PSD2 (Directive (EU) 2015/2366)**.
- **Must disclose to clients:**
    - **Terms & conditions** of payment services.
    - **Applicable national law & client rights**.
    - **Whether services are provided directly or via a third party**.

Why?
Ensures **transparency** and **regulatory compliance** in payment processing.

4. Exemptions (Paragraph 5)

- **Does not apply to:**
    - **Electronic money institutions (EMIs)**.
    - **Payment institutions (PIs)**.
    - **Credit institutions (banks)**.
- **Reason:** These entities already follow **similar safeguarding rules** under **PSD2, EMD2, or banking laws**.

Article 71: Complaints-Handling Procedures for Crypto-Asset Service Providers

Article 71 establishes **mandatory rules** for how **Crypto-Asset Service Providers (CASPs)** must handle **client complaints**, ensuring **fair treatment, transparency, and accountability**.

Key Requirements of Article 71

1. Mandatory Complaints-Handling Procedures (Paragraph 1)

- CASPs must implement **clear, effective, and transparent** complaint procedures.
- These procedures must be **publicly disclosed** (e.g., on the CASP's website).

Why?
Ensures clients know how to raise issues and trust that complaints will be addressed fairly.

2. Free Complaint Submission (Paragraph 2)

- Clients must be able to **file complaints for free** (no fees or barriers).

Why?
Prevents CASPs from discouraging complaints through financial disincentives.

3. Complaint Awareness & Record-Keeping (Paragraph 3)

- CASPs must **inform clients** of their right to complain.
- Must provide a **complaint template** (standardized form).
- Must **keep records** of all complaints and **actions taken**.

Why?

- Ensures **easy access** to complaint mechanisms.
- Helps regulators **monitor CASP conduct**.

4. Fair & Timely Investigation (Paragraph 4)

- Complaints must be **investigated fairly and promptly**.
- CASPs must **inform clients of the outcome** within a **reasonable time**.

Why?
Prevents delays or dismissals of valid complaints.

5. ESMA's Regulatory Technical Standards (Paragraph 5)

- **ESMA & EBA** will develop **detailed complaint-handling rules** by **30 June 2024**, including:
    - **Standardized complaint templates**.
    - **Procedures for resolution timelines**.
- The **EU Commission** will adopt these as binding standards.

Why?
Ensures **consistent enforcement** across the EU.

Article 72: Identification, prevention, management and disclosure of conflicts of interest

Article 72 mandates that **Crypto-Asset Service Providers (CASPs)** must **identify, prevent, manage, and disclose conflicts of interest** to protect clients and ensure market integrity.

Key Requirements of Article 72:

1. Policies & Procedures to Manage Conflicts (Paragraph 1)

CASPs must establish **written policies** to handle conflicts between:

- **Themselves and:**
    - Shareholders/members
    - Related parties (e.g., subsidiaries, controlling entities)
    - Management & employees
    - Clients
- **Between clients** (e.g., front-running, preferential treatment).

Examples of Conflicts in Crypto:

- A CEX **trading against its own clients** (proprietary trading).
- A custodian **lending out clients' crypto** without consent.
- A broker **prioritizing high-volume traders** over retail users.

2. Public Disclosure of Conflicts (Paragraph 2 & 3)

- CASPs must **publish conflicts of interest** on their website in a **clear, accessible format**.
- Disclosures must include:
    - **Nature & sources** of conflicts (e.g., affiliated trading desks).
    - **Measures taken to mitigate** them (e.g., Chinese walls, restricted access).
- Must be **detailed enough** for clients to make **informed decisions**.

Why?
Prevents **hidden biases** (e.g., a CEX promoting its own token over competitors).

3. Annual Review & Updates (Paragraph 4)

- CASPs must **review their conflict policies at least yearly** and **fix gaps**.

Why?
Ensures policies stay effective as the business evolves (e.g., new services, partnerships).

4. ESMA's Regulatory Technical Standards (Paragraph 5)

- **ESMA & EBA** will draft **detailed rules** by **30 June 2024** on:
    - **Minimum standards** for conflict policies (scaled to business size/services).
    - **Disclosure formats & methodology** (what must be disclosed and how).
- The **EU Commission** will adopt these as binding rules.

Why?
Ensures **uniform enforcement** across the EU.

Article 73: Outsourcing

Article 73 establishes **strict rules** for **outsourcing** by CASPs to ensure **operational resilience, accountability, and regulatory compliance** even when third parties are involved.

Key Requirements of Article 73

1. Conditions for Outsourcing (Paragraph 1)

CASPs **remain fully responsible** for outsourced functions and must ensure:

Condition	Explanation	Why It Matters
(a) No delegation of responsibility	The CASP is still legally accountable for outsourced tasks.	Prevents CASPs from blaming third parties for failures.
(b) No change in client obligations	Clients' rights and the CASP's duties remain unchanged.	Ensures consumer protection isn't weakened.
(c) No impact on authorization	Outsourcing must not violate the CASP's license terms.	Prevents regulatory arbitrage.
(d) Third-party cooperation with regulators	Outsourcers must allow **supervisory access** (e.g., audits, on-site checks).	Ensures regulators can oversee risks.
(e) CASP retains oversight capability	Must keep **expertise/resources** to monitor third parties.	Avoids over-reliance on vendors.
(f) Direct access to outsourced data	CASPs must be able to audit third-party operations.	Prevents data hiding or manipulation.
(g) GDPR compliance	Third parties must meet **EU data protection standards**.	Protects client privacy and security.

Example:
If a CASP outsources **wallet custody** to a third party, it must still **ensure security** and **allow regulators to inspect** the vendor.

2. Outsourcing Policy (Paragraph 2)

CASPs must have a **written outsourcing policy** covering:

- **Risk assessment** (due diligence on vendors).
- **Contingency plans** (backups if the vendor fails).
- **Exit strategies** (how to switch providers if needed).

Why?
Prevents **service disruptions** (e.g., if a cloud provider goes down).

3. Written Agreements (Paragraph 3)

- **Contracts must define** roles, responsibilities, and **termination rights**.
- CASPs must **retain the power to end agreements** if the vendor underperforms.

Example:
A CASP using a **KYC provider** must have a contract allowing it to **switch vendors** if compliance lapses occur.

4. Regulatory Access (Paragraph 4)

- **CASPs & third parties must share records** with regulators upon request.
- Ensures **outsourced activities comply with MiCAR**.

Why?
Prevents CASPs from hiding risky outsourcing (e.g., using offshore unregulated vendors).

Article 74: Orderly Wind-Down of Crypto-Asset Service Providers (CASPs)

Article 74 mandates that **CASPs must have a structured plan** to **wind down operations safely** without harming clients or disrupting markets. This is critical to prevent **disorderly collapses** (like FTX) that could lead to **client asset losses or systemic risks**.

Key Requirements of Article 74

1. Wind-Down Plan Obligations

CASPs providing services under **Articles 75-79** (e.g., custody, trading, staking) must:

- **Prepare a documented wind-down plan** under national law.
- Ensure the plan covers:
    - **Continuity or recovery of critical activities** (e.g., allowing clients to withdraw funds).
    - **Minimizing economic harm to clients** (no sudden freezes or losses).

Example:
A failing crypto exchange must have a plan to:
✓ Allow **orderly client withdrawals**.
✓ Transfer **custodied assets** to another licensed provider.
✓ Notify **regulators and users** transparently.

2. Objectives of the Plan

The wind-down plan must ensure:

- **No undue harm to clients** (e.g., preventing asset stranding).
- **Compliance with national insolvency laws** (e.g., EU member state regulations).
- **Clear steps for critical operations** (e.g., how nodes, wallets, or trading systems will be maintained during transition).

Why?
Prevents **chaotic shutdowns** where clients lose access to funds (e.g., Mt. Gox, Celsius).

3. Regulatory & Client Protection Focus

- CASPs must **prove the plan's feasibility** to regulators during licensing.
- The plan must be **regularly reviewed and updated** (e.g., annually).

Penalties for Non-Compliance:

- **Fines or license revocation** if no credible plan exists.
- **Forced administration** if regulators intervene.

Chapter 3: Obligations for specific Crypto-Asset Services

Article 75: Providing Custody & Administration of Crypto-Assets on Behalf of Clients

Article 75 establishes **strict rules** for **Crypto-Asset Service Providers (CASPs)** offering **custody and administration services** (e.g., crypto wallets, asset safekeeping). It ensures **client asset protection, transparency, and operational security**.

Key Requirements of Article 75

1. Mandatory Client Agreement (Paragraph 1)

CASPs must have a **written agreement** with clients, including:

- **Parties' identities** (CASP & client).
- **Description of services** (e.g., cold storage, staking).
- **Custody policy** (how assets are secured).
- **Authentication & communication methods** (e.g., 2FA, support channels).
- **Security measures** (e.g., multi-sig, encryption).
- **Fees & charges**.
- **Applicable law** (jurisdiction for disputes).

Why?
Ensures **clients understand risks and protections**.

2. Register of Client Positions (Paragraph 2)

- CASPs must maintain a **real-time ledger** of:
    - Each client's **crypto holdings**.
    - **All transactions** (movements must be recorded immediately).

Why?
Prevents **misappropriation or accounting errors** (e.g., FTX's commingled funds).

3. Custody Policy (Paragraph 3)

- Must have **internal rules** to minimize risks of:
    - **Theft** (fraud, hacking).
    - **Loss** (negligence, key mismanagement).
- **Summary must be shared** with clients upon request.

Example:
A CASP using **cold storage** must document:
✓ **Who holds private keys**.
✓ **How backups are secured**.

4. Handling Crypto-Asset Rights (Paragraph 4)

- CASPs must **facilitate client rights** (e.g., staking rewards, governance votes).
- If **blockchain upgrades** (e.g., forks) create new assets, clients **must receive them** unless agreed otherwise.

Why?
Prevents CASPs from **withholding forked coins** (e.g., Bitcoin Cash after a BTC fork).

5. Client Reporting (Paragraph 5)

- **Quarterly statements** (electronic) showing:
    - Crypto balances.
    - Transaction history.
    - Asset valuations.
- **Immediate alerts** for actions requiring client response (e.g., withdrawal requests).

Why?
Ensures **transparency** and **dispute resolution**.

6. Asset Return Procedures (Paragraph 6)

- CASPs must have a **clear process** to **return client assets promptly** (e.g., if services end).

Why?
Prevents **FTX-style freezes** where users couldn't withdraw.

7. Segregation of Client Assets (Paragraph 7)

- **Client assets must be:**
    - **Held separately** from the CASP's own funds.
    - **Legally protected** from creditors in insolvency.
    - **Operationally distinct** (no commingling).

Why?
Ensures **client funds aren't used for trading or loans** (like Celsius did).

8. Liability for Losses (Paragraph 8)

- CASPs are **liable for losses due to their negligence** (e.g., hacks, mismanagement).
- **Liability cap** = **market value at time of loss**.
- **Exclusions**: Losses from **external blockchain failures** (e.g., network outages).

Example:
If a CASP's hot wallet is hacked, it must **compensate clients**.

9. Sub-Custody Rules (Paragraph 9)

- If using **third-party custodians**, they must be **MiCAR-authorized**.
- Clients **must be informed** of sub-custody arrangements.

Why?
Prevents **risky outsourcing** (e.g., unregulated offshore custodians).

Article 76: Operation of a Trading Platform for Crypto-Assets

Article 76 establishes **comprehensive rules** for **Crypto-Asset Service Providers (CASPs)** operating **trading platforms** (e.g., centralized exchanges like Binance or decentralized platforms with order books). It ensures **fair, transparent, and resilient markets** while preventing **market abuse, fraud, and conflicts of interest**.

Key Requirements of Article 76

1. Operating Rules for Trading Platforms (Paragraph 1)

CASPs must establish **clear, transparent rules** covering:

- **Admission of crypto-assets** (due diligence, AML checks).

- **Exclusion criteria** (e.g., privacy coins without traceability).
- **Non-discriminatory access** (fair participation for all traders).
- **Order execution policies** (objective, non-discretionary).
- **Suspension/delisting conditions** (e.g., low liquidity, fraud).
- **Settlement procedures** (timely crypto/fiat settlements).

Critical Provision:

- **No trading of crypto-assets without a published white paper** (where required by MiCAR).

Why?
Prevents **scam tokens** from being listed (e.g., pump-and-dump schemes).

2. Suitability Assessment for Crypto-Assets (Paragraph 2)

Before listing, CASPs must assess:

- **Technical reliability** (e.g., smart contract audits).
- **Issuer reputation** (team track record, fraud risks).
- **Association with illicit activities** (e.g., money laundering).

Example:
An exchange must **vet a new DeFi token** by checking:
✓ Audit reports (e.g., CertiK).
✓ Team anonymity risks.
✓ Past regulatory actions.

3. Ban on Anonymous Crypto-Assets (Paragraph 3)

- **No trading of privacy coins** (e.g., Monero, Zcash) **unless**:
    - **Holders can be identified** (compliance with AML rules).

Why?
Aligns with **EU anti-money laundering (AML) laws**.

4. Language Requirements (Paragraph 4)

- Operating rules must be in:
    - **Home Member State's official language** (or English/financial sector standard).
    - **Host Member State's language** if operating cross-border.

Why?
Ensures **legal clarity** for regulators and users.

5. Prohibition on Proprietary Trading (Paragraph 5)

- **Exchanges cannot trade against clients** (no "market making" by the platform itself).

Why?
Prevents **conflicts of interest** (e.g., front-running client orders).

6. Matched Principal Trading (Paragraph 6)

- **Allowed only with client consent** (must inform regulators).

- **No hidden dealing**—must remain a neutral matching service.

Example:
A platform acting as a **broker-dealer** must disclose its role.

7. Trading System Resilience (Paragraph 7)

Platforms must ensure:

- **Capacity for high trading volumes** (no crashes during volatility).
- **Order safeguards** (e.g., rejecting erroneous trades).
- **Market abuse detection** (e.g., wash trading, spoofing).
- **Business continuity plans** (e.g., backup servers).

Why?
Prevents **"Robinhood-style" outages** during market stress.

8. Market Abuse Reporting (Paragraph 8)

- **Must report suspicious activity** (e.g., insider trading, pump-and-dump).

Why?
Aligns with **EU Market Abuse Regulation (MAR)**.

9. Transparency in Pricing (Paragraphs 9-11)

- **Real-time publication** of:
    - Bid/ask prices.
    - Trade volumes & timestamps.
- **Free delayed data** (15 mins old) in **machine-readable format**.

Why?
Ensures **fair price discovery** (no hidden spreads).

10. Settlement Deadlines (Paragraph 12)

- **On-chain settlements within 24 hours**.
- **Off-chain settlements by end of day**.

Why?
Prevents **delays in fund delivery** (e.g., FTX withholding withdrawals).

11. Fair Fee Structures (Paragraph 13)

- **No manipulative incentives** (e.g., rebates for excessive trading).

Example:
Ban on **"zero-fee" trading** that encourages market distortion.

12. Order Book Record-Keeping (Paragraph 15)

- **Store all order data for 5+ years** (regulator access required).

Why?
Helps investigate **market manipulation**.

13. ESMA Technical Standards (Paragraph 16)

- **ESMA will standardize**:
    - **Transparency data formats** (e.g., how trades are reported).
    - **Order book record-keeping**.
- Deadline: **30 June 2024**.

Article 77: Exchange of Crypto-Assets for Funds or Other Crypto-Assets

Article 77 regulates **crypto-asset exchange services** (e.g., brokerages, OTC desks, and instant exchange platforms) to ensure **fair pricing, transparency, and non-discriminatory access** for clients.

Key Requirements of Article 77:

1. Non-Discriminatory Commercial Policy (Paragraph 1)

- CASPs must define a **clear policy** stating:
    - **Which clients they serve** (e.g., retail, institutional).
    - **Conditions for transactions** (e.g., KYC tiers, minimum trade sizes).
- **No arbitrary refusal of service** (must apply rules uniformly).

Example:
A crypto brokerage cannot **deny service to a retail trader** without justification if they meet stated criteria.

2. Transparent Pricing (Paragraph 2)

- CASPs must **publicly disclose**:
    - **Fixed prices** (e.g., "1 BTC = €30,000") **or**
    - **Pricing methodology** (e.g., "price = CoinGecko spot + 1% fee").
    - **Exchange limits** (e.g., "Max €10,000 per trade").

Why?
Prevents **hidden markups** or **surprise fees** (common in OTC trades).

3. Execution at Published Prices (Paragraph 3)

- **Orders must be filled at the displayed price** when the order is finalized.
- CASPs must **clearly explain** when an order becomes **binding** (e.g., after user confirmation).

Example:
If a user agrees to swap **1 ETH for €2,000**, the exchange cannot later adjust the rate unless predefined conditions apply (e.g., slippage limits).

4. Post-Trade Transparency (Paragraph 4)

- CASPs must **publish aggregated trade data**, including:
    - **Transaction volumes**.
    - **Execution prices**.

Why?
Helps users **verify fair execution** and detect **price manipulation**.

Article 78: Execution of Orders for Crypto-Assets on Behalf of Clients

Article 78 establishes **strict best execution standards** for **Crypto-Asset Service Providers (CASPs)** that execute client orders (e.g., brokers, trading desks). It ensures clients receive **fair, transparent, and optimal trade execution** while preventing **conflicts of interest or misuse of order information**.

Key Requirements of Article 78

1. Best Execution Obligation (Paragraph 1)

CASPs must take **all necessary steps** to achieve the **best possible result** for clients, considering:

- **Price** (most favorable rate).
- **Costs** (fees, spreads).
- **Speed & likelihood of execution**.
- **Settlement conditions**.
- **Size & nature of the order**.

Exception:

- If a client gives **specific instructions** (e.g., "sell at €30,000, no matter what"), the CASP is **not liable** for suboptimal execution.

Why?
Prevents brokers from **routing orders to inferior venues** for kickbacks.

2. Order Execution Policy (Paragraph 2)

CASPs must implement a **written policy** ensuring:

- **Prompt, fair, and efficient execution**.
- **No front-running or misuse of client orders** (e.g., trading ahead).

Example:
A broker must document how it **prioritizes liquidity sources** (e.g., Binance vs. Uniswap).

3. Client Disclosure & Consent (Paragraph 3)

- CASPs must **clearly explain** their execution policy to clients **in simple terms**.
- **Client consent** is required (either per trade or as a general agreement).

Why?
Ensures clients understand **how their trades are handled**.

4. Compliance Proof (Paragraph 4)

- CASPs must **demonstrate execution quality** to:
    - **Clients** (upon request).
    - **Regulators** (during audits).

Example:
A broker must show **trade logs** proving orders were filled at the best available price.

5. Off-Exchange Execution (Paragraph 5)

- If orders are executed **outside trading platforms** (e.g., OTC desks), CASPs must:
    - **Inform clients**.
    - **Obtain explicit consent** (general or per transaction).

Why?
Prevents **hidden OTC deals** that may disadvantage clients.

6. Ongoing Monitoring & Updates (Paragraph 6)

- CASPs must **regularly review execution quality** and:
    - **Fix deficiencies** (e.g., switching to better liquidity providers).
    - **Notify clients of material changes** (e.g., new fee structures).

Why?
Ensures **continuous improvement** in execution standards.

Article 79: Placing of Crypto-Assets

Article 79 regulates **crypto-asset placement services**, where CASPs (Crypto-Asset Service Providers) act as intermediaries to distribute crypto-assets (e.g., ICOs, token sales, or private placements) on behalf of issuers. The rules ensure **transparency, fair pricing, and conflict-of-interest management** to protect investors.

Key Requirements of Article 79:

1. Mandatory Pre-Agreement Disclosures (Paragraph 1)

Before entering into a placement agreement, CASPs must disclose to issuers (or their representatives):

Disclosure	Explanation	Purpose
(a) Type of placement	Whether the placement is **guaranteed** (e.g., underwritten) or **best-efforts**.	Prevents misleading fundraising expectations.
(b) Transaction fees	All costs charged to the issuer (e.g., commission, listing fees).	Ensures **no hidden charges**.
(c) Timing, process & pricing	Expected schedule, allocation method, and pricing mechanism.	Avoids **last-minute changes** disadvantaging investors.
(d) Targeted purchasers	Whether placement is for **retail, institutional, or specific investors**.	Prevents **improper marketing** (e.g., selling high-risk tokens to unsophisticated buyers).

Consent Requirement:

- The issuer must **agree in writing** to these terms before the placement begins.

Why?
Ensures **both parties align on expectations** (e.g., no surprise fees or delays).

2. Conflict-of-Interest Management (Paragraph 2)

CASPs must implement **specific procedures** to handle conflicts, such as:

Conflict Scenario	Mitigation Required
(a) Placing assets with own clients	Disclose if the CASP prioritizes its clients over others.
(b) Over/under-pricing	Prove pricing is fair (e.g., independent valuation).
(c) Incentives from issuers	Disclose any **kickbacks** (monetary or non-monetary).

Example:
A CASP must **publicly disclose** if it receives **bonus tokens** for selling a project's ICO.

Article 80: Reception and Transmission of Orders for Crypto-Assets on Behalf of Clients

Article 80 regulates **Crypto-Asset Service Providers (CASPs)** that receive and transmit client orders (e.g., crypto brokers, trading intermediaries) to ensure **fair order routing, no conflicts of interest, and protection of client information**.

Key Requirements of Article 80

1. Order Transmission Procedures (Paragraph 1)

CASPs must:

- **Promptly and accurately route client orders** to:
    - A **trading platform** (e.g., Binance, Kraken).
    - Another **authorized crypto-asset service provider**.
- Ensure **no unnecessary delays** or **intentional misrouting**.

Why?
Prevents brokers from **delaying orders** to profit from price changes.

2. Ban on Preferential Order Routing (Paragraph 2)

- CASPs **cannot accept** any form of **compensation** (money, discounts, or other benefits) for:
    - **Directing orders to specific platforms** (e.g., payment for order flow).
    - **Favoring certain service providers**.

Example:
A broker cannot receive **kickbacks from Exchange X** for sending all client orders there.

Why?
Prevents **conflicts of interest** that harm clients (e.g., routing to inferior platforms for profit).

3. Protection of Client Order Information (Paragraph 3)

- CASPs must:
    - **Not misuse pending order data** (e.g., front-running).
    - **Prevent employees from exploiting insider knowledge** (e.g., trading ahead of clients).

Example:
A broker's employee cannot **buy Bitcoin** just before executing a large client buy order.

Why?
Protects clients from **information asymmetry and market abuse**.

Article 81: Providing Advice on Crypto-Assets and Portfolio Management

Article 81 establishes **strict suitability and transparency rules** for **Crypto-Asset Service Providers (CASPs)** offering **investment advice** or **portfolio management** services. It ensures that crypto recommendations align with clients' financial situations, risk tolerance, and investment objectives while preventing conflicts of interest.

1. Suitability Assessment (Paragraph 1)

Before providing advice or managing a portfolio, CASPs must assess whether a crypto-asset or service is suitable for a client based on:

- **Knowledge & experience** in crypto investments.
- **Investment objectives** (short-term vs. long-term).
- **Risk tolerance** (ability to handle volatility).
- **Financial situation** (ability to bear losses).

Why?
Prevents **mis-selling** (e.g., recommending high-risk DeFi tokens to risk-averse investors).

2. Disclosure of Advice Nature (Paragraph 2)

CASPs must inform clients **before providing advice** whether it is:

- **(a) Independent** (unbiased, broad market analysis).
- **(b) Non-independent** (limited to certain crypto-assets, possibly due to issuer ties).

Example:
A CEX-affiliated advisor must disclose if they only recommend **their own exchange's tokens**.

3. Independent Advice Requirements (Paragraph 3)

If a CASP claims **independence**, it must:

- **(a) Assess a diverse range of crypto-assets** (not just those from affiliated issuers).
- **(b) Not accept monetary/non-monetary benefits** (e.g., kickbacks from projects).

Exception:

- **Minor non-monetary benefits** (e.g., research tools) are allowed if they **enhance service quality** and are **fully disclosed**.

Why?
Prevents **biased recommendations** (e.g., shilling tokens for hidden rewards).

4. Cost Transparency (Paragraph 4)

CASPs must disclose **all costs**, including:

- **Advice fees** (if applicable).
- **Crypto-asset costs** (e.g., spreads, transaction fees).
- **Third-party payments** (e.g., referral commissions).

Why?
Ensures clients understand **total expenses** before investing.

5. Portfolio Management Conflicts (Paragraph 5)

Portfolio managers **cannot accept fees/benefits** from:

- **Token issuers** (e.g., incentives to hold certain assets).
- **Third parties** (e.g., referral bonuses).

Why?
Prevents **misaligned incentives** (e.g., favoring high-commission tokens).

6. Non-Independent Advice & Inducements (Paragraph 6)

If advice is **non-independent**, CASPs can accept inducements **only if**:

- **(a) They enhance service quality**.
- **(b) They don't impair fair treatment**.
- **Full disclosure** is required (nature, amount, or calculation method).

Example:
A **CEX-affiliated advisor** can receive bonuses for promoting in-house tokens **if clearly disclosed**.

7. Advisor Competency (Paragraph 7)

- **Advisors must have necessary knowledge/competence**.
- **EU Member States** will publish **assessment criteria**.

Why?
Prevents **untrained staff** giving risky advice.

8. Client Information Collection (Paragraph 8)

CASPs must gather **detailed client profiles**, including:

- **Investment experience** (crypto & traditional).
- **Risk tolerance** (conservative vs. aggressive).
- **Financial capacity** (ability to absorb losses).

Why?
Ensures **personalized recommendations**.

9. Mandatory Risk Warnings (Paragraph 9)

Clients must be warned that:

- **(a) Crypto prices are volatile**.
- **(b) Total loss is possible**.

- **(c) Liquidity risks exist** (some tokens can't be sold easily).
- **(d) No investor compensation** (unlike bank deposits).
- **(e) No deposit guarantee** (unlike traditional banking).

Why?
Ensures **informed consent** before investing.

10. Suitability Policies (Paragraph 10)

CASPs must implement **procedures** to:

- **Collect reliable client data**.
- **Assess suitability accurately**.

Why?
Prevents **automated approvals without checks**.

11. No Unsuitable Recommendations (Paragraph 11)

If:

- **Clients refuse to provide info**, or
- **Crypto-assets are deemed unsuitable**,
  CASPs **must not recommend or manage** those assets.

Why?
Prevents **reckless advice** (e.g., pushing leverage trading to retirees).

12. Regular Suitability Reviews (Paragraph 12)

- **At least every 2 years**, CASPs must **reassess client suitability**.
- **More frequent updates** if circumstances change (e.g., market crashes).

Why?
Ensures **ongoing alignment** with client needs.

13. Suitability Reports (Paragraph 13)

After assessments, CASPs must provide **electronic reports** detailing:

- **Updated suitability analysis**.
- **How advice matches client goals**.

Why?
Gives clients **transparency & recourse** if advice is mismatched.

14. Portfolio Management Statements (Paragraph 14)

Portfolio managers must send **quarterly statements** (or provide **real-time online access**) showing:

- **Performance review**.
- **Updated suitability assessment**.

Why?
Ensures **clients can track investments** and adjust strategies.

15. ESMA Guidelines (Paragraph 15)

By **30 December 2024**, ESMA will issue guidelines on:

- **Advisor competency standards**.
- **Suitability assessment criteria**.
- **Portfolio statement formats**.

Why?
Ensures **uniform EU-wide implementation**.

Article 82: Providing Transfer Services for Crypto-Assets on Behalf of Clients

Article 82 regulates **Crypto-Asset Service Providers (CASPs)** that offer **transfer services** (e.g., crypto payment processors, wallet-to-wallet transfer providers). It ensures **transparency, security, and legal clarity** in crypto transactions.

1. Mandatory Client Agreement (Paragraph 1)

Before providing transfer services, CASPs must sign a **written agreement** with clients, including:

(a) Identity of Parties

- Names and details of **both the CASP and the client**.

(b) Description of Transfer Service

- **How transfers are executed** (e.g., on-chain, off-chain, batch processing).
- **Supported blockchains & assets** (e.g., Bitcoin, Ethereum).
- **Processing times** (e.g., instant, delayed for security checks).

(c) Security Systems

- **Authentication methods** (e.g., 2FA, multi-sig).
- **Fraud prevention measures** (e.g., address whitelisting, transaction monitoring).
- **Cold/hot wallet storage policies**.

(d) Fees

- **Explicit breakdown of costs** (e.g., network fees, service charges).
- **No hidden fees** (must be disclosed upfront).

(e) Applicable Law

- **Jurisdiction governing the agreement** (e.g., German law for a German CASP).

Why?

- Prevents **misunderstandings** about service terms.
- Ensures **legal enforceability** in disputes.

2. ESMA & EBA Guidelines (Paragraph 2)

- **ESMA & EBA** will issue **guidelines** on:

    - **Procedures & policies** for transfer services.
    - **Client rights** (e.g., refunds, dispute resolution).
- Deadline: **Not specified**, but expected post-MiCAR implementation.

Expected Guidelines May Cover:
✓ **Transaction reversal policies** (e.g., handling erroneous transfers).
✓ **Complaint resolution mechanisms**.
✓ **Minimum security standards** (e.g., encryption, key management).

Why?
Ensures **consistent EU-wide standards** for crypto transfers.

Chapter 4: Acquisition of CASPs

Article 83: Assessment of Proposed Acquisitions of Crypto-Asset Service Providers (CASPs)

Article 83 of Regulation (EU) 2023/1114 (MiCA) outlines the process for assessing proposed acquisitions of qualifying holdings in Crypto-Asset Service Providers (CASPs) within the European Union. It establishes a structured framework to ensure that significant ownership changes in CASPs are transparent, compliant with regulatory standards, and do not undermine the stability or integrity of the crypto-asset market. Below is a detailed explanation of each paragraph, ensuring no aspect is missed.

1. Notification of Proposed Acquisition (Paragraph 1)

- **Who Must Notify**: Any natural or legal person (or persons acting together), referred to as the "proposed acquirer," who decides to:
    - Acquire a **qualifying holding** in a CASP, either directly or indirectly, or
    - Increase an existing qualifying holding so that their ownership of voting rights or capital reaches or exceeds **20%, 30%, or 50%**, or
    - Acquire enough of a holding to make the CASP their **subsidiary**.
- **What is a Qualifying Holding?**: While not explicitly defined in this paragraph, it typically refers to a significant stake that grants influence over the CASP (aligned with thresholds like 10% or more, as seen in other EU financial regulations, but here specified as triggering at 20%+).
- **Notification Process**:
    - The proposed acquirer must notify the **competent authority** (NCA) of the CASP in writing.
    - The notification must include:
        - The **size of the intended holding** (e.g., percentage of voting rights or capital).
        - **Information required** by regulatory technical standards (RTS) set out by the European Commission under **Article 84(4)**. (This likely includes details like the acquirer's identity, financial status, and intentions—explained further in Article 84).
- **Purpose**: Ensures regulators are aware of significant ownership changes that could affect the CASP's operations, governance, or compliance with MiCA.

Example: A French company decides to buy 25% of a German CASP's shares. It must notify BaFin (Germany's NCA) in writing with the required details.

2. Notification of Disposal of Qualifying Holding (Paragraph 2)

- **Who Must Notify**: Any natural or legal person who decides to:
    - **Dispose** of a qualifying holding in a CASP, either directly or indirectly, or
    - **Reduce** their qualifying holding so that their voting rights or capital fall below **10%, 20%, 30%, or 50%**, or
    - Reduce their holding so that the CASP **ceases to be their subsidiary**.

- **Notification Process**:
    - The person must notify the competent authority **in writing** before disposing of the holding.
    - The notification must include:
        - The **size of the holding** they plan to dispose of or reduce.
- **Additional Requirement**: The person must also inform the NCA of their decision to reduce the holding below the specified thresholds or end the subsidiary relationship.
- **Purpose**: Allows regulators to monitor significant reductions in ownership that might affect the CASP's stability or control structure.

Example: A Spanish investor holding 35% of a Dutch CASP decides to sell enough shares to drop below 20%. They must notify the Dutch NCA (AFM) beforehand.

3. Acknowledgment of Receipt (Paragraph 3)

- **Timeline**: The competent authority must acknowledge receipt of the acquisition notification (from Paragraph 1) **within 2 working days** of receiving it.
- **Method**: Acknowledgment must be in writing.
- **Purpose**: Provides a formal starting point for the assessment process, ensuring transparency and a clear timeline for the acquirer.

Example: BaFin receives an acquisition notice on Monday and must send a written acknowledgment by Wednesday.

4. Assessment Period (Paragraph 4)

- **Timeline**: The competent authority has **60 working days** to assess the proposed acquisition, starting from the date of the written acknowledgment (Paragraph 3).
- **Scope**: The assessment covers:
    - The proposed acquisition itself (from Paragraph 1).
    - The information provided per the RTS under Article 84(4).
- **Notification**: When acknowledging receipt, the NCA must inform the proposed acquirer of the **exact expiry date** of the 60-day assessment period.
- **Purpose**: Sets a clear, predictable timeframe for regulators to evaluate the acquisition's impact on the CASP and the market.

Example: If BaFin acknowledges receipt on April 4, 2025, it must complete the assessment by approximately June 30, 2025 (accounting for weekends and holidays), and inform the acquirer of this deadline.

5. Consultation with Other Authorities (Paragraph 5)

- **Requirement**: During the assessment, the competent authority **may consult**:
    - Competent authorities for **anti-money laundering and counter-terrorist financing (AML/CFT)**.
    - **Financial intelligence units (FIUs)**.
- **Obligation**: The NCA must **duly consider** the views of these consulted bodies.

- **Purpose**: Ensures a holistic review, particularly for AML/CFT risks, leveraging expertise from specialized regulators.

Example: BaFin consults Germany's FIU (FIU Deutschland) to check if the acquirer has any AML red flags.

6. Requests for Additional Information (Paragraph 6)

- **Request Process**:
    - The competent authority **may request additional information** from the proposed acquirer if needed to complete the assessment.
    - Requests must be:
        - Made **before the assessment is finalized**.
        - No later than the **50th working day** of the 60-day period.
        - In writing, specifying the additional info needed.
- **Suspension of Assessment**:
    - The 60-day assessment period is **suspended** until the additional information is received.
    - Suspension lasts up to **20 working days**.
    - If the acquirer is outside the EU or regulated by a third-country law, the suspension can be extended to **30 working days**.
- **Limits**: Further requests for info or clarification after the initial request **do not suspend** the timeline again.
- **Purpose**: Allows NCAs to gather necessary data while balancing efficiency with thoroughness; longer suspension for non-EU acquirers reflects potential delays in cross-border coordination.

Example: On Day 45, BaFin requests financial statements. The clock stops for up to 20 days (or 30 if the acquirer is in the U.S.) until the info is provided.

7. Decision to Oppose Acquisition (Paragraph 7)

- **Timeline**: If the competent authority decides to **oppose** the acquisition, it must notify the proposed acquirer:
    - **Within 2 working days** of the decision.
    - Before the end of the 60-day period (or extended period if suspended under Paragraph 6).
- **Notification**: The decision must include **reasons** for opposing the acquisition.
- **Purpose**: Ensures prompt communication and transparency if the acquisition is deemed risky or non-compliant.

Example: BaFin opposes an acquisition on Day 58 due to AML concerns and notifies the acquirer by Day 60 with a detailed explanation.

8. Automatic Approval (Paragraph 8)

- **Rule**: If the competent authority does not oppose the acquisition by the end of the 60-day period (or extended period under Paragraph 6), the acquisition is **deemed approved**.

- **Purpose**: Prevents indefinite delays; provides certainty to acquirers if no objections are raised.

Example: If BaFin doesn't act by June 30, 2025 (end of the 60-day period), the acquisition is automatically approved.

9. Maximum Period for Concluding Acquisition (Paragraph 9)

- **Authority**: The competent authority **may set a maximum period** for the proposed acquirer to complete the acquisition.
- **Flexibility**: The NCA can **extend this period** if appropriate.
- **Purpose**: Ensures the acquisition is finalized in a timely manner, preventing prolonged uncertainty, while allowing flexibility for complex deals.

Example: BaFin approves an acquisition and sets a 6-month deadline to finalize it, later extending it to 9 months due to legal delays.

Article 84: Content of the Assessment of Proposed Acquisitions

Article 84 of Regulation (EU) 2023/1114 (MiCA) specifies the criteria and procedural details for assessing proposed acquisitions of Crypto-Asset Service Providers (CASPs) as outlined in Article 83(4). It ensures that competent authorities (NCAs) evaluate the suitability of acquirers and the financial viability of acquisitions in a consistent, transparent, and prudential manner. Below is a detailed explanation of each paragraph, covering all aspects without omission.

1. Assessment Criteria (Paragraph 1)

- **Context**: When conducting the 60-day assessment under Article 83(4), the competent authority must evaluate the **suitability of the proposed acquirer** and the **financial soundness of the proposed acquisition** (as per Article 83(1)).
- **Criteria**: The assessment is based on the following five specific factors:
    - **(a) Reputation of the Proposed Acquirer**:
        - The NCA examines the acquirer's integrity and track record, including any history of legal, regulatory, or ethical issues.
        - Purpose: Ensures the acquirer is trustworthy and unlikely to destabilize the CASP or the market.
        - Example: A history of fraud convictions would negatively impact reputation.
    - **(b) Reputation, Knowledge, Skills, and Experience of Directors**:
        - Focuses on individuals who will **direct the CASP's business** post-acquisition (e.g., new board members or executives appointed as a result of the acquisition).
        - Evaluates their:
            - Reputation (similar to the acquirer's).
            - Knowledge, skills, and experience in crypto-asset services or related fields.
        - Purpose: Confirms that leadership will be competent and reputable.
        - Example: A director with no crypto expertise might raise concerns.

- **(c) Financial Soundness of the Proposed Acquirer**:
  - Assesses the acquirer's financial stability, particularly in relation to the CASP's planned business activities.
  - Considers liquidity, capital adequacy, and ability to support the CASP's operations.
  - Purpose: Ensures the acquisition won't strain the CASP's finances.
  - Example: An acquirer with heavy debt might be deemed unsound.
- **(d) Ongoing Compliance with MiCA Title V**:
  - Verifies that the CASP will **comply** (and continue to comply) with MiCA's requirements post-acquisition (e.g., capital reserves, governance, client protection under Title V).
  - Purpose: Protects the CASP's operational integrity and market compliance.
  - Example: If the acquirer plans to cut compliance staff, this could jeopardize adherence.
- **(e) Money Laundering/Terrorist Financing (ML/TF) Risks**:
  - Investigates whether there are **reasonable grounds to suspect**:
    - ML/TF (as defined in Directive (EU) 2015/849, Articles 1(3) and 1(5)) is occurring or has occurred in connection with the acquisition, or
    - The acquisition could **increase ML/TF risk**.
  - Purpose: Prevents illicit activities from infiltrating the crypto market.
  - Example: An acquirer linked to a high-risk jurisdiction might trigger suspicion.

- **Purpose**: These criteria ensure a holistic review of the acquisition's impact on the CASP's stability, governance, and compliance.

2. Grounds for Opposition (Paragraph 2)

- **Rule**: The competent authority can **oppose the proposed acquisition** only if:
  - There are **reasonable grounds** based on the criteria in Paragraph 1 (a-e), or
  - The information provided under Article 83(4) is **incomplete or false**.
- **Details**:
  - Opposition must be justified by specific failings (e.g., poor reputation, ML/TF risks, or financial instability).
  - Incomplete/false info (e.g., missing financial statements or fabricated data) also warrants rejection.
- **Purpose**: Limits NCA discretion to objective, evidence-based decisions, ensuring fairness while protecting the market.
- **Example**: If an acquirer hides a criminal record (false info) or has insufficient funds (criterion c), the NCA can oppose.

3. Prohibition of Additional Conditions (Paragraph 3)

- **Rule**: Member States are **prohibited** from:

    - Imposing **prior conditions** on the level of qualifying holding required (e.g., mandating a minimum stake beyond MiCA thresholds).
    - Allowing NCAs to assess the acquisition based on the **economic needs of the market** (e.g., whether the market "needs" the acquisition).
- **Purpose**: Ensures a uniform, prudential approach across the EU, preventing Member States from adding arbitrary barriers or economic protectionism.
- **Example**: Germany cannot require an acquirer to buy 25% instead of 20%, nor reject an acquisition because the crypto market is "saturated."

4. ESMA and EBA's Role in Regulatory Technical Standards (Paragraph 4)

- **Responsibility**:
    - The **European Securities and Markets Authority (ESMA)**, working closely with the **European Banking Authority (EBA)**, must develop **draft regulatory technical standards (RTS)**.
    - These RTS specify the **detailed content of the information** required for the assessment under Article 83(4).
- **Requirements for RTS**:
    - The information must be:
        - **Relevant** for a prudential assessment (focused on financial stability and compliance).
        - **Proportionate** and **adapted** to the nature of the acquirer and acquisition (e.g., tailored to individual vs. corporate acquirers, or small vs. large stakes).
- **Timeline**: ESMA must submit these draft RTS to the **European Commission** by **June 30, 2024**.
- **Delegation**:
    - The Commission has the power to **adopt these RTS** as a supplement to MiCA.
    - Adoption follows **Articles 10-14 of Regulation (EU) No 1095/2010** (ESMA's founding regulation), which outline the process for technical standards (e.g., consultation, Commission approval).
- **Purpose**: Standardizes the information NCAs need (e.g., financial statements, acquirer background) to ensure consistency and efficiency across the EU.
- **Example**: The RTS might require a corporate acquirer to submit audited accounts but only a personal affidavit for an individual.

Chapter 5: Significant CASPs

Article 85: Identification of Significant Crypto-Asset Service Providers (CASPs)

Article 85 of Regulation (EU) 2023/1114 (MiCA) establishes the criteria and procedures for identifying "significant" Crypto-Asset Service Providers (CASPs) within the European Union, along with their associated supervisory obligations. This designation triggers enhanced oversight by both national competent authorities (NCAs) and the European Securities and Markets Authority (ESMA) to ensure market stability and consumer protection for large-scale CASPs. Below is a detailed explanation of each paragraph, ensuring no aspect is omitted.

1. Definition of a Significant CASP (Paragraph 1)

- **Criteria**: A CASP is classified as "significant" if it has:
    - **At least 15 million active users** in the EU, on average, over one calendar year.
- **Calculation Method**:
    - The average is determined by calculating the **daily number of active users** throughout the previous calendar year and then averaging those daily figures.
    - "Active users" is not explicitly defined here but typically implies users who engage in transactions or services (e.g., trading, custody) rather than just registered accounts.
- **Purpose**: Identifies CASPs with a large user base that could pose systemic risks to the EU crypto market if mismanaged, requiring heightened supervision.
- **Example**: A CASP with 20 million daily active users in January, 14 million in June, and 16 million in December of 2024 would average above 15 million, qualifying as significant.

2. Notification Process (Paragraph 2)

- **Obligation of CASPs**:
    - CASPs must **notify their competent authority** (NCA) within **2 months** of reaching the 15 million active user threshold.
    - This notification is self-reported by the CASP based on its internal data.
- **Role of the NCA**:
    - The NCA reviews the notification to confirm whether the threshold in Paragraph 1 is met.
    - If the NCA agrees, it **notifies ESMA** of the CASP's significant status.
- **Purpose**: Ensures timely identification and escalation of significant CASPs to ESMA for coordinated oversight.
- **Example**: A French CASP hits 15 million users in March 2025 and notifies the ACPR by May 2025. The ACPR verifies and informs ESMA.

3. Supervisory Updates to ESMA (Paragraph 3)

- **Annual Updates**:
    - The NCAs of the home Member States of significant CASPs must provide **ESMA's Board of Supervisors** with **annual updates** on supervisory developments.
    - These updates cover:
        - **(a) Ongoing or Concluded Authorizations**:

        - Refers to the authorization process under **Article 59** (e.g., initial licensing or amendments).
    - **(b) Ongoing or Concluded Withdrawals of Authorizations**:
        - Refers to withdrawal processes under **Article 64** (e.g., due to non-compliance or inactivity).
    - **(c) Exercise of Supervisory Powers**:
        - Specific powers listed in **Article 94(1)**, first subparagraph, points (b), (c), (e), (f), (g), (y), and (aa), which include actions like:

            (b) Requesting information.
            (c) Conducting investigations.
            (e) Requiring remedial actions.
            (f) Imposing restrictions.
            (g) Suspending services.
            (y) Issuing warnings.
            (aa) Imposing fines.

- **Optional Updates**:
    - NCAs **may provide more frequent updates** or notify ESMA **before decisions** related to points (a), (b), or (c).
    - This allows real-time coordination if urgent issues arise.
- **Clarification**: This is **without prejudice** to NCAs' responsibilities under MiCA, meaning NCAs retain primary supervisory authority, but ESMA is kept informed.
- **Purpose**: Ensures ESMA has a comprehensive, up-to-date view of significant CASPs' regulatory status and supervisory actions for EU-wide consistency.
- **Example**: Germany's BaFin annually reports to ESMA that a significant CASP's authorization was amended (Article 59) and fines were imposed (Article 94).

4. Exchange of Views at ESMA (Paragraph 4)

- **Process**: The updates provided under Paragraph 3 (especially the optional, pre-decision notifications) **may** lead to an **exchange of views** at ESMA's Board of Supervisors.
- **Nature**: This is not mandatory ("may") but provides a forum for discussion among ESMA members.
- **Purpose**: Facilitates collaboration and alignment among NCAs and ESMA on handling significant CASPs, especially for complex or cross-border issues.
- **Example**: BaFin notifies ESMA of a potential withdrawal (Article 64) in advance, prompting a discussion at ESMA on its EU-wide implications.

5. ESMA's Powers (Paragraph 5)

- **Authority**: Where appropriate, ESMA can exercise its powers under **Articles 29, 30, 31, and 31b** of **Regulation (EU) No 1095/2010** (ESMA's founding regulation).
- **Specific Powers**:
    - **Article 29**: Coordination functions (e.g., fostering supervisory cooperation).
    - **Article 30**: Peer reviews (e.g., assessing NCA performance).

    - **Article 31**: General supervisory convergence (e.g., issuing guidelines).
    - **Article 31b**: Binding mediation (e.g., resolving disputes between NCAs).
- **Condition**: Use of these powers is discretionary ("where appropriate"), based on ESMA's judgment of need.
- **Purpose**: Empowers ESMA to intervene or coordinate if significant CASPs pose risks or if NCAs' supervision diverges, ensuring a unified EU approach.
- **Example**: ESMA conducts a peer review (Article 30) if a significant CASP's NCA is lax on Article 94 enforcement.