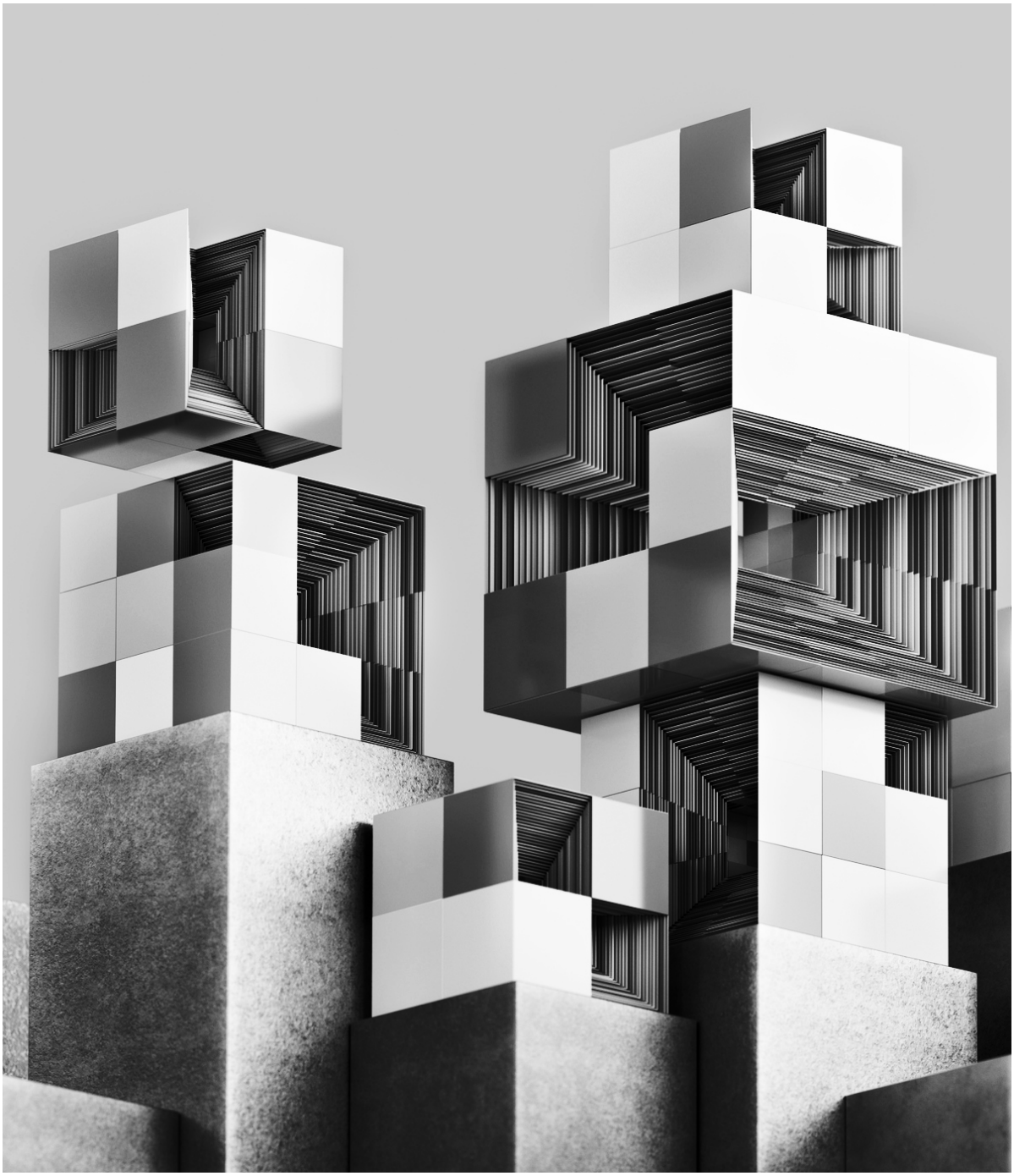
A&O SHEARMAN



MiCAR under the *microscope*

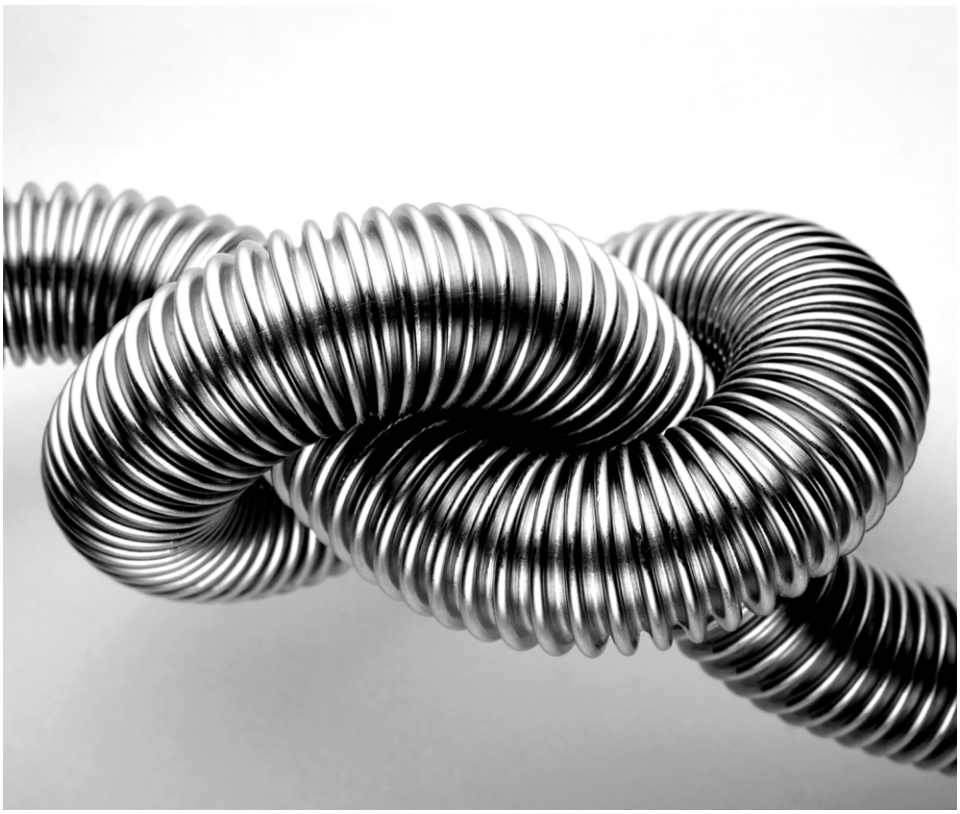
PART 5: REGULATORY REQUIREMENTS APPLICABLE TO CASPS

Part 5: Regulatory requirements applicable to CASPs

The Regulation (EU) 2023/1114 on Markets in Crypto-assets (**MiCAR**) has further expanded the panel of regulated entities by introducing the regulatory status of crypto-asset service providers (**CASPs**). According to the taxonomy introduced by MiCAR, CASPs are defined as legal persons or other undertakings engaging in the provision of one or more crypto-asset services (**CAS**) to clients on a professional basis.[1]

This edition of our "MiCAR under the microscope" series analyses the general regulatory requirements applicable to CASPs providing CAS within the European Union. In particular, after analysing the regime provided for by MiCAR to govern CASPs' operations, irrespective of their business model and operativity size, this publication will then discuss the additional and more stringent requirements that the European legislator has provided for specific categories of CASPs identified by virtue of their size and/or core business of the activities they (intend to) provide within the European Union.

As better detailed below, many of the obligations applicable to CASPs under MiCAR are largely inspired by the obligations applicable to investment firms under Directive 2014/65/EU on markets in financial instruments (**MiFID**) or Directive 2015/2366 on payment services (**PSD2**).



[1] Please refer to the A&O, now A&O Shearman, fourth instalment of this bulletin series for an insight into this brand new regulated entity and a specific focus on the main steps of the CASP authorisation and passporting regime (available here).

1. Regulatory requirements applicable to *CASPs*

1.1 GOVERNANCE REQUIREMENTS[2]

(A) FIT AND PROPER REQUIREMENTS APPLICABLE TO THE MANAGEMENT BODY, PERSONNEL AND SHAREHOLDERS OF CASPs

Following an approach already (widely) used by the European policymakers under the MiFID framework, the fit and proper regime envisaged under MiCAR is three-fold and consists of:

(i) the fit and proper requirements applicable to members of the management body and to any shareholders (or other members) having a qualified holdings in CASPs;

(ii) rules of conduct: CASPs are called on to implement adequate internal policies and procedures to ensure a sufficient level of compliance with the requirements set forth under limb (i) above; and

(iii) reporting requirements to the national competent regulator(s) as to any changes in the composition of the management body.

(B) BACKUP, RESPONSE AND RECOVERY PLAN

CASPs are required to ensure the continuity and regularity in the performance of their services.

In light of the technological and digital features and implications of their core business (consisting of engaging in activities relating to assets issued, created and transferred in a pure and native digital format as tokens), CASPs' operational resilience may be seriously challenged by ICT risks (i.e. those risks stemming from *inter alia* the use of a network and information system and which materialise as an adverse effect in the digital or physical environment).

In light of the above, the adequacy of the measures and arrangements established and implemented by CASPs in order to ensure business continuity and regularity is strictly related to, and dependent on, CASPs' compliance with the requirements and provisions set out in Regulation (EU) 2022/2554 (**DORA**) and its relevant implementing acts and regulations which, in line with the phase-in regime, at the date of this bulletin are in the process of adoption both at European and national level.

Among others, the requirements set forth by DORA require that a CASP should:

- periodically test its ICT business continuity plan and its ICT response and recovery plan, especially for critical functions;
- develop and document backup policies and procedures (supported by backup ICT systems which should be segregated from the source ICT system) as well as recovery procedures and methods;
- carry out a business impact analysis of its exposure to severe business disruption;
- have a crisis management function and keep accessible records of its activity before and during disruption events; and
- report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents.

[2] Please note that – since this series is intended to focus on the main changes and regulatory implications that MiCAR is about to introduce within the European Union for EU and/or non-EU crypto-market operators – we do not analyse regimes and / or pieces of legislation which, although being of direct relevance for and application to the crypto-market operators, fall outside the MiCAR framework. For example, but without limitation, for this publication we have not taken into account AML rules and related issues stemming from the so-called Travel Rule Regulation (i.e. Regulation (EU) 2023/1113).

(C) RECORD KEEPING REQUIREMENTS

Similar to investment firms under MiFID, in accordance with Article 68(9) of MiCAR, CASPs are required to keep records of all crypto-asset services, activities, orders and transactions that they undertake.

(D) OUTSOURCING REQUIREMENTS

MiCAR also provides specific requirements and conditions that CASPs should comply with when implementing outsourcing arrangements. MiCAR's approach with regards to outsourcing arrangements is largely aligned to that followed under already-existing financial services regulations. As such, MiCAR aims at preventing, or at least minimising, to the extent possible, the risk that the recourse to these arrangements may impact CASPs' operational resilience or may result in a full delegation of responsibilities and, consequently, lack of efficient supervisory activities.

To prevent the abovementioned risks, MiCAR provides that outsourcing agreements should be duly covered by a specific outsourcing policy, detailing inter alia contingency plans and exit strategies, and shall include a de minimis (pre-identified) set of rights and obligations of the CASP and any delegated third-party.

To avoid any (potential) impact on the business continuity and regularity on the side of the CASPs, no material restrictions or limitations should be placed on the rights of CASPs to terminate the outsourcing agreements.

All the relevant information necessary to assess the compliance of the outsourced activities with the authorisation and operating conditions for CASPs should be made available upon request to the competent authorities. Consequently, CASPs should ensure that their compliance with MiCAR outsourcing requirements is properly documented.

1.2 CONDUCT OF BUSINESS

(A) ACTING IN THE BEST INTERESTS OF THE CLIENT

As is the case with investment firms under MiFID, when conducting business, CASPs are under the obligation to act in the best interests of the client.

To this end:

(i) the information they provide to clients, including marketing communications, should be clear and not misleading;

(ii) a CASP's policy on pricing, costs and fees should be publicly available in a prominent place on its website along with information on the climate-related impact of the crypto-assets in relation to which they provide services; and

(iii) a CASP should warn its clients of the various risks to which they may be exposed by transacting in crypto-assets.

(B) MANAGING CONFLICTS OF INTEREST

CASPs are under an obligation to implement and maintain effective policies and procedures to identify, prevent, manage and disclose conflicts of interest.

These policies and procedures are to be reviewed at least annually and conflicts of interest are to be disclosed on the website of the CASP.

(C) COMPLAINTS HANDLING

CASPs must establish and maintain effective and transparent complaint handling procedures and make them publicly available.

Complaints may be filed by CASPs' clients free of charge, filling-in a standard template, and shall be investigated by the relevant CASP in a timely and fair manner. The outcome of the complaint shall be disclosed to the client within a reasonable period, although the black-letter does not currently envisage a firm deadline by which a complaint should be handled by the CASP and reported to the relevant client.

(D) SAFEGUARDING OF CUSTOMER'S CRYPTO-ASSETS AND FUNDS

In the event that a CASP holds crypto-assets belonging to a client or the means of access to such crypto-assets, it is under the obligation to safeguard the client's ownership rights, especially in the case of the CASP's insolvency, and not to use the client's crypto-assets for its own account.

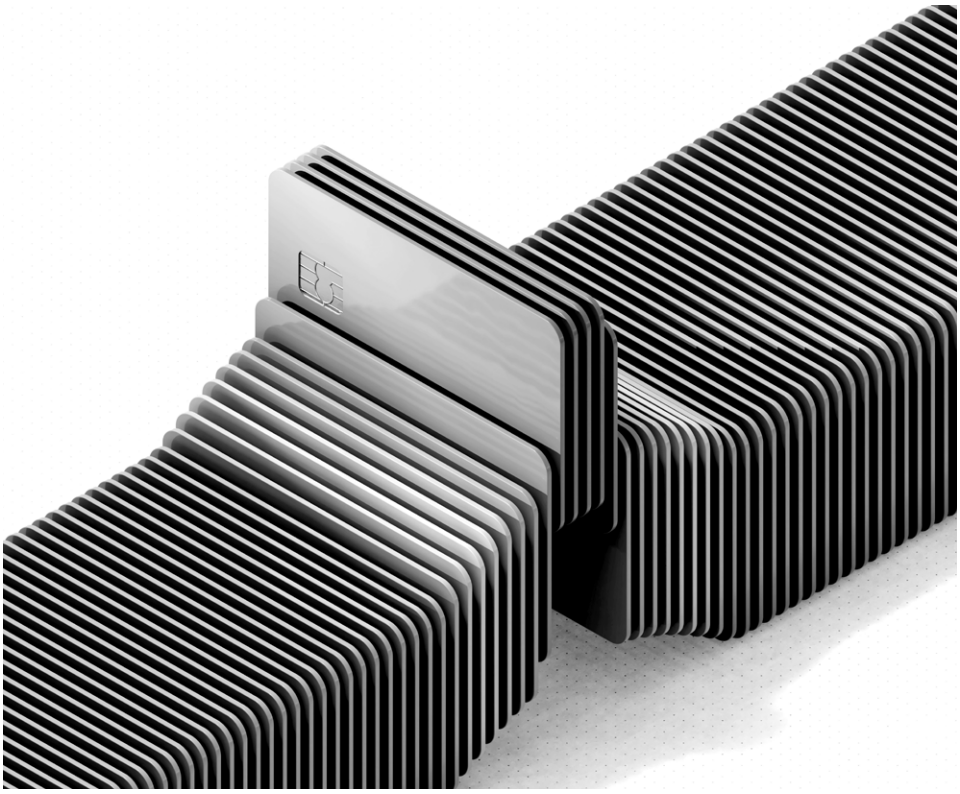
Where a CASP receives customer funds (other than e-money tokens), it is under the obligation to safeguard those funds by the end of the business day following the day of their receipt, by placing them in a segregate safeguarding account opened with a credit institution or a central bank.

As this regime basically replicates the approach already followed at a European level under other preexisting financial services regulations, CASPs that are authorised under Article 60 of MiCAR as being financial entities providing CAS remain subject to the regulatory regime set forth under that separate EU legal framework.

2. Additional regulatory requirements applicable to *certain CASPs*

In addition to the de minimis set of rules applicable to all CASPs as a direct consequence of their regulatory status (as summarised above), MiCAR envisages a second layer of provisions (in terms of requirements, reporting obligations and duties) which will be tailored to (and therefore their application is modular on) the CAS performed by the CASP and / or the size of the CASP's operativity (i.e. the so-called significant CASPs).

Below is a brief summary of the main requirements applicable to CASPs depending on the specificities (and related risks) associated with a specific CAS or stemming from the size of the CASPs in terms of their client base (and consequently activity volume).



2.1 ENHANCED SUPERVISION OF SIGNIFICANT CASPs

A CASP is considered to be significant where it reaches on average 15 million active users in a calendar year. Within two months of crossing that threshold, the CASP must notify its competent authority.

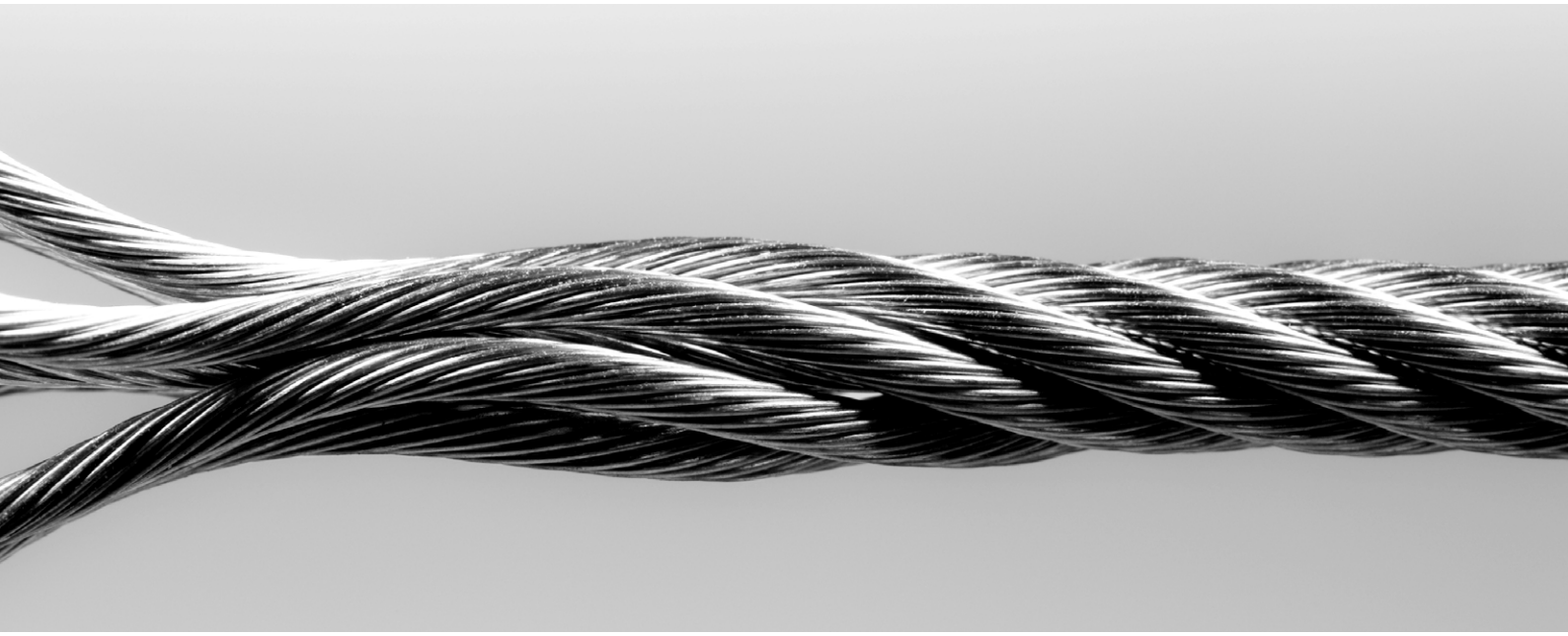
CASPs that are considered significant are subject to enhanced monitoring from competent authorities which are also under an obligation to provide additional information and reporting to the European Securities and Markets Authority (**ESMA**) in relation to the CASP.

2.2 SPECIFIC OBLIGATIONS BY TYPE OF SERVICE PROVIDED BY THE CASP

TYPE OF CAS	NON-EXHAUSTIVE LIST OF KEY ADDITIONAL REQUIREMENTS
Custody and administration of crypto-assets on behalf of clients	CASPs are required to comply, inter alia, with the following requirements: **(i)** legally and operationally segregate the crypto-assets held on the behalf of the client from the crypto-assets held for its own account; **(ii)** keep a register of the positions opened for each client and record every movement[3]; **(iii)** establish a custody policy to ensure the safekeeping or the control of or the means to access the crypto-assets. Such custody policy is also to be made available to the client; **(iv)** ensure that necessary procedures are in place to return crypto-assets to the client as soon as possible; **(v)** conclude an agreement with the client which shall include at least the specific elements listed by MiCAR; and **(vi)** have in place a plan that is appropriate to support an orderly wind-down of its activities under applicable national law and ensure the continuity or recovery of any critical activities performed. A CASP may make use of another CASP for custody purposes only to the extent that these entities are authorised pursuant to Article 59 of MiCAR. Furthermore, the client should be informed thereof.
Operating a trading platform for crypto-assets	CASPs are required to comply, inter alia, with the following requirements: **(i)** set-out and implement clear and transparent operating rules, which include inter alia non-discriminatory access policies and prior screening as to the proper compliance of the crypto-assets to be admitted to trading with the operating rules; **(ii)** settle the crypto-asset transaction on the distributed ledger less than 24 hours after the execution of the transaction on the platform; **(iii)** make public certain information regarding the bids and transactions related to crypto-assets traded on its trading platforms (e.g. bid and ask prices the depth of trading interests at those prices, the price, volume and time of the transactions executed); **(iv)** keep records related to all orders in crypto-assets for at least 5 years; and **(v)** have in place a plan that is appropriate to support an orderly wind-down of its activities under applicable national law and ensure the continuity or recovery of any critical activities performed. CASPs are finally prohibited from dealing on own account on their own platform and may engage in matched principal trading only subject to specific conditions.
Exchange of crypto-assets for other funds or other crypto-assets	CASPs are required to comply, inter alia, with the following requirements: **(i)** establish a commercial policy that states, in particular, the type of targeted clients and the conditions that shall be met by such clients to be eligible to transact with the CASP; **(ii)** to avoid any manipulation on the price of crypto-assets, public disclosure requirements pertaining to inter alia the firm price of the crypto-asset that the CASPs propose to exchange for funds or other crypto-assets and any limit thereof; and information regarding transaction volume; **(iii)** have in place a plan that is appropriate to support an orderly wind-down of their activities under applicable national law and ensure the continuity or recovery of any critical activities performed.

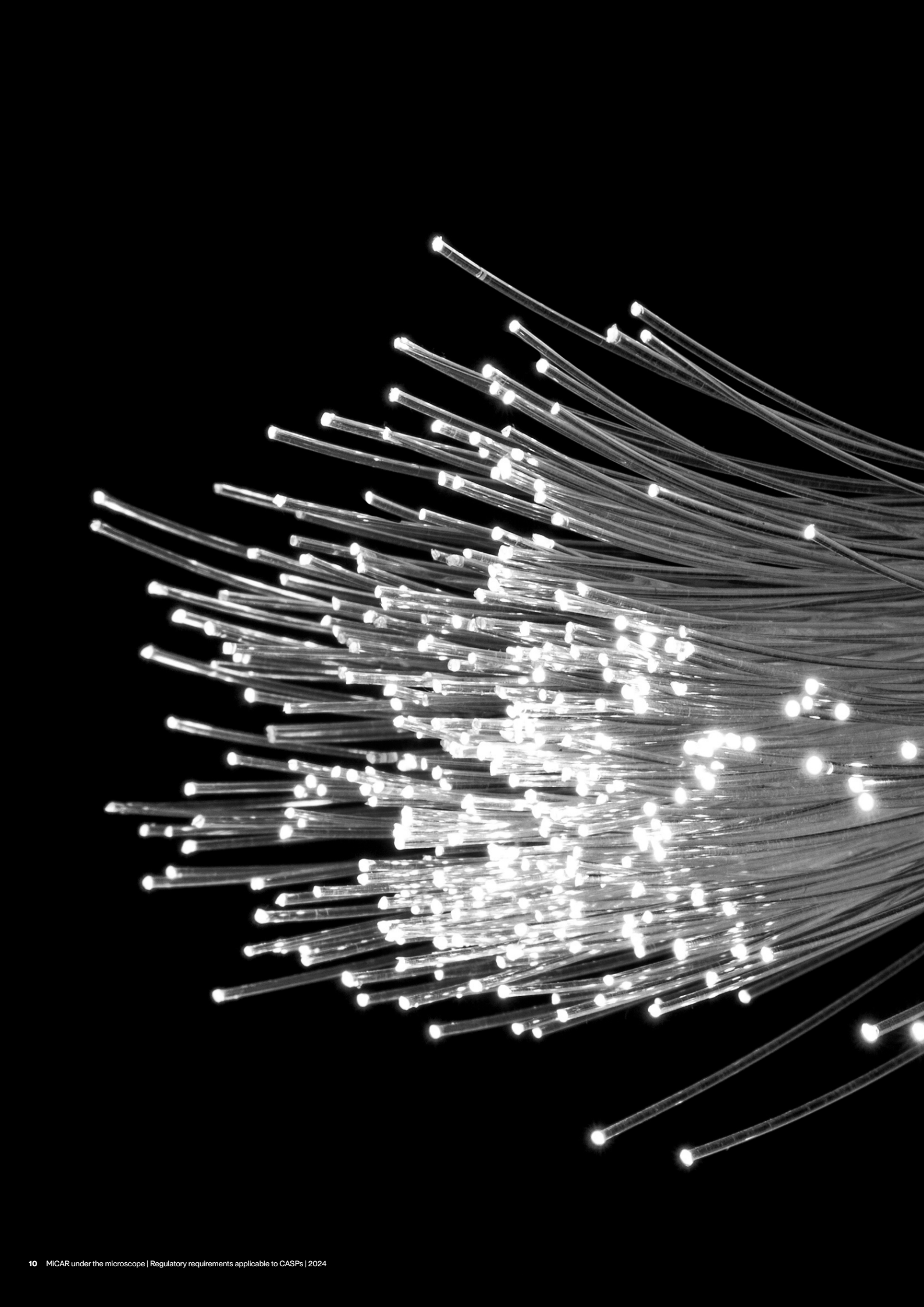
[3] These records should be made available to the client upon request and at least every three months.

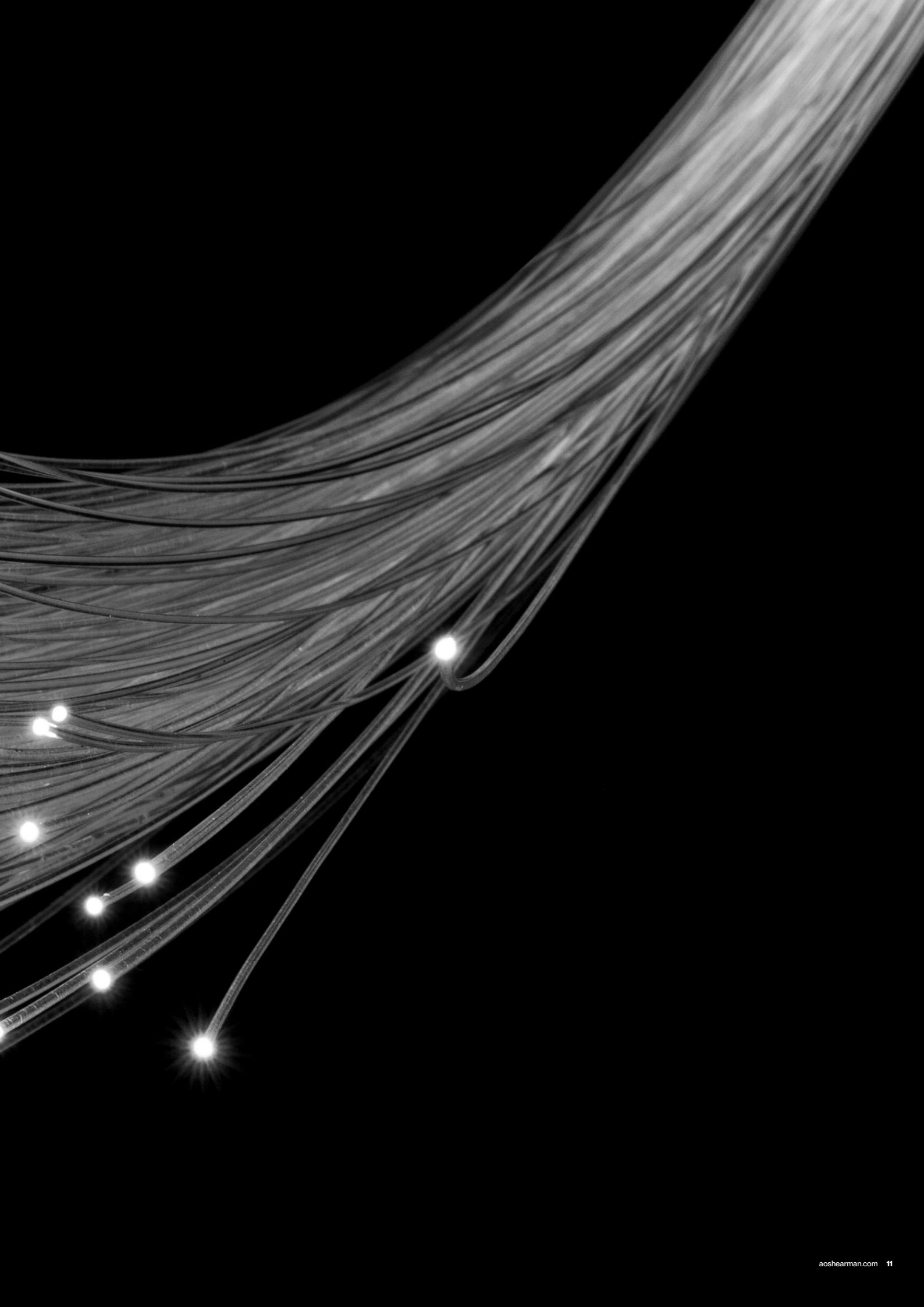
TYPE OF CAS	NON-EXHAUSTIVE LIST OF KEY ADDITIONAL REQUIREMENTS
Execution of orders for crypto-assets on behalf of clients	Similar to the framework designed by the European legislator for serving MiFID purposes, CASPs are primarily required to act in a fair and transparent manner in order to ensure the best possible result for their clients while executing their orders. In practical terms, this means that CASPs are expected to implement a specific execution policy, also governing the circumstances and conditions to be met to execute orders outside their trading platform. The effectiveness of the execution policy and relevant implementing arrangements shall be duly monitored. Period reporting and disclosure requirements are then envisaged in favour of clients both in terms of content of the execution policy and evidence of how clients' orders have been effectively executed in line with that policy and implementing internal arrangements.
Placing of crypto-assets	Before any agreement with a person seeking admission to trading, the CASP must communicate certain information. Specific conflicts of interest rules are also applicable to the placing of crypto-assets. Finally, CASPs should have in place a plan that is appropriate to support an orderly wind-down of their activities under applicable national law and ensure the continuity or recovery of any critical activities performed.
Reception and transmission of orders related to crypto-assets	CASPs are required to establish and implement procedures and arrangements that provide for prompt and proper transmission of a client's orders to a trading platform or to another CASP. CASPs are also barred from: • Receiving any form of remuneration, discount or benefit for routing the client's order through a particular trading platform / CASP (i.e. the inducements regime); • misusing information on pending orders (and must take appropriate steps to prevent such misuse by employees).



TYPE OF CAS	NON-EXHAUSTIVE LIST OF KEY ADDITIONAL REQUIREMENTS
Providing advice on crypto-assets and providing portfolio management of crypto-assets	With a view to ensuring adequate protection to end-users, also in light of the high price volatility and underlying complex risks which have so far characterised trading in crypto-assets, CASPs providing advice on and /or portfolio management of crypto-assets are primarily expected to carefully assess the suitability of investments / trading activities in crypto-assets for their clients, duly taking into account a wide range of factors including, inter alia, their knowledge and experience in the crypto-space or their investment objectives. Similar to MiFID investment advice, there is an obligation to inform the client whether the advice is provided on an independent basis and/or based on a broad or restricted analysis of different crypto-assets. CASPs should also ensure that the person providing the advice is qualified to do so. Specific disclosure requirements towards clients – which may vary depending on the nature of the advice provided (based on a dependent or independent basis) – apply. This includes, subject to some exceptions, the disclosure of periodic (at least every 3 months) statements of the portfolio management activities carried out on behalf of clients. CASPs are also barred from accepting and retaining any fees, commissions or any monetary or non-monetary benefits from issuers, offerors or persons seeking admission to trading or any third party in relation to the provision of portfolio management of crypto-assets to their clients.
Providing transfer services for crypto-assets on behalf of clients	The agreement between a CASP and its client should include at least the elements prescribed by MiCAR.

Please note that the information included in this alert only and strictly focuses on the provisions laid down by MiCAR and does not extent to also cover the content and further requirements provided for by the secondary level acts and legislations the European regulators (and eventually the European legislators) published and enacted shortly before the present publication.





Global presence

A&O Shearman is an international legal practice with nearly 4,000 lawyers, including some 800 partners, working in 29 countries worldwide. A current list of A&O Shearman offices is available at aoshearman.com/en/global-coverage.

A&O Shearman means Allen Overy Shearman Sterling LLP and/or its affiliated undertakings. Allen Overy Shearman Sterling LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen Overy Shearman Sterling LLP (SRA number 401323) is authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen Overy Shearman Sterling LLP or a director of Allen Overy Shearman Sterling (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen Overy Shearman Sterling LLP's affiliated undertakings. A list of the members of Allen Overy Shearman Sterling LLP and of the non-members who are designated as partners, and a list of the directors of Allen Overy Shearman Sterling (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

A&O Shearman was formed on May 1, 2024 by the combination of Shearman & Sterling LLP and Allen & Overy LLP and their respective affiliates (the legacy firms). This content may include material generated and matters undertaken by one or more of the legacy firms rather than A&O Shearman.

aoshearman.com

ROW
Disclaimer
CS2405_CDD-77901_ADD-114322