

Financial Law Review

No. 42 (2)/2026

UNIVERSITY OF GDAŃSK • MASARYK UNIVERSITY • PAVEL JOZEF ŠAFÁRIK UNIVERSITY
<http://www.ejournals.eu/FLR>

MAGDALENA FEDOROWICZ*

SUPERVISION OF CRYPTO-ASSET SERVICE PROVIDERS¹

Abstract

The purpose of this study is to analyse the regulations concerning CASPs and outsourcing in the CA market from the perspective of supervisory regulations and to answer the question of the completeness and coherency of the adopted regulations, especially with regard to CASPs from third countries, under the normative conditions of Article 61 of MiCA. The point of reference for the considerations presented in this article is, first, the principle of financial stability related to CASP activities, second, the principle of digital security formulated in the DORA Regulation. The conclusions of the study can be summarised as follows: there are functional links between the supervisory regulations for CASPs under MiCAR and DORAR, which are of key importance for digital security and resilience in the crypto-asset market, whilst Article 61 of MiCAR provides for highly flexible, from the perspective of client protection under-regulated provisions of client acquisition.

Key words: CASP, Crypto-assets, DORAR, MiCAR, reverse solicitation

JEL Classification: K20, K22, K23, K24

* Magdalena, Fedorowicz, Professor, Department of Financial Law, Faculty of Law and Administration, Adam Mickiewicz University in Poznań, Poland.
Contact email: magdalena.fedorowicz@amu.edu.pl, ORCID: 0000-0002-5578-5170.

¹ Parts of this article were presented at the 25th *International Scientific Conference PUBLIC FINANCE, TAXATION AND FINANCIAL REGULATION IN TIMES OF MULTI-CRISIS*, 24-26th September 2025, in Košice, Slovakia.

1. Introduction

The adoption of the MiCA Regulation (Regulation (EU) 2023/1114, hereinafter referred to as MiCA or MiCAR) significantly changes the regulatory situation on the crypto-asset (hereinafter: CA) market (crypto-asset market: hereinafter CAM) [Hrabčák, Štrkolec 2024]. In addition to introducing supervision over the issuance and trading of CA and regulating the specific process of tokenisation of the CAM, supervision has also been extended to crypto-asset service providers (hereinafter CASP) [Srokosz 2023: 436-444].

The purpose of this study is to analyze the regulations concerning CASPs and outsourcing in the CAM from the perspective of supervisory regulations and to answer the question of the completeness and coherency of the adopted regulations, especially with regard to CASPs from third countries, under the normative conditions of Article 61 of MiCA. The point of reference for the considerations presented in this article is, first, the principle of financial stability related to CASP activities, second, the principle of digital security formulated in the DORA regulation (Regulation (EU) 2022/2554, hereinafter referred to as the DORA Regulation or DORAR), linked, among other things, to critical ICT third-party service providers, also ICT third-party service provider established in a third country (hereinafter DORAR), and thirdly, the principle of consumer protection in the CAM, reconstructed from these two regulations.

It will also be important to answer questions about the tasks of supervisory authorities at national and EU level, as well as the existence of platforms for mutual cooperation between supervisory authorities in Member States and third countries on CASPs and their activities². It is also worth noting that although the study will consider and assess the provisions relating to the objectives, tasks and competences of supervisory authorities mainly from the perspective of financial stability and financial security, the comments, conclusions and evaluation will also address the effectiveness of customer protection in the CAM interacting with CASPs. The latter is all the more important given that there are no guarantee funds in the CAM [Fedorowicz 2024: 61-75]. Furthermore, an important issue from the point of view of customer protection in the CAM is that of CASP from third countries (Art. 61 MiCA), both from the perspective of the MiCA and the DORA Regulations,

² Polish law implementing MiCA on the crypto-asset market have been vetoed twice by the President.

as well as the regulation of outsourcing institution in the CAM contained in MiCAR.

The theses of this study are, firstly, that there is disproportionate and overly flexible supervision of third-country CASPs compared to the supervisory regulations for CASPs based in the EU and, secondly, that it is the supervisory authorities, mainly national ones, that have the difficult task of ensuring stability, digital security and customer protection in the CAM, in particular by means of instruments influencing the content of legal relationships between CASPs, outsourcers or ICT service providers and financial entities.

The research method adopted in this study is the dogmatic-legal method.

2. The crypto-asset market from an EU supervisory perspective, including in particular the organisation of CASPs

The MiCAR introduces a number of provisions regulating the supervision of the organisation of the CAM, including the supervision of entities providing CA services [Fedorowicz, 2021: 75-88]. As is well known, this is the first comprehensive EU regulation of the CAM organisation, with the full implementation of MiCA additionally requiring Member States to adopt laws implementing the MiCAR. In addition, it should be noted that the MiCAR is also functionally linked to the implementation of the DAC-8 Directive on the exchange of information on CA between competent authorities (also AML authorities).

There is an important link between MiCA and DORA, as DORA's provisions on risk and digital resilience apply to issuers, CASPs and CA platform operators.

The CASP regulation in MiCA is particularly important for financial security, especially in situations where the service provider is based outside the EU, and also for customers who would use the services or products of CA providers based outside the EU.

Under MiCA, supervision of CA providers is subject to the obligation to obtain a CASP licence from the national supervisor (Article 59 MiCA). Given that the MiCAR also provides for a category of significant CASPs, this supervision is carried out directly by the EU supervisor once the existence of a significant CASP has been established or the entity has self-qualified as a significant CASP [Buttigieg, 2025]. It is important that CASPs prudential safeguards are checked during the licensing process (Article 67 MiCA), as

this is particularly important for future CASPs customers who are not banks or investment firms.

As always when regulating areas previously unregulated by EU or national legislation, the problem arises of optimal regulation [Buttigieg, Cuyle, 2024:233-243] that complies with the principles of proportionality, stability [Fedorowicz 2025: 1029-1039] and freedom and transparency in the provision of CA services, as well as competitiveness vis-à-vis third countries or (other EU countries with varying degrees of liberalism in their implementation of EU law) on the one hand, and on the other hand, stability and financial security and regulatory convergence [Asschemann 2023: 489-500] ensured by means of cooperation between national and EU supervisors and not centralisation of direct supervision by ESMA [Buttigieg, 2026:49-58] and also necessary collaboration with FIUs. It can be argued that the CAM, as a market without strong customer protection, a highly decentralised market, without guarantee funds, highly volatile with many investment risks, requires clear and consistent supervisory regulation, and the shape of the first and second government draft law implementing MiCA in Poland was generally well in line with the relatively clear assumptions of the MiCAR and the implementation of the DAC-8 directive and of the future implementation of new AML regulations.

The organisation and regulation of CASPs in MiCA largely mirrors the normative provisions of MiFID II with regard to investment service providers. This similarity is evident, for example, in the requirement for CASPs to obtain authorisation to provide services and the obligation to act honestly, fairly and professionally in accordance with the best interests of their clients (Article 66 MiCA). The principle of transparency of activities, protection through client information, the principle of best execution, and warning clients about risks are the main elements designed to counteract mis-selling and misleading clients, which have been repeatedly analysed in regulatory theory and practice in relation to investment services under MiFID II.

3. Supervisory instruments over CASP in the light of MiCA and DORA regulations

As already mentioned, pursuant to Article 59 in conjunction with Article 63 of the MiCAR, CASPs are subject to the legitimate requirement to obtain authorisation from national supervisors – or, in the case of significant CASPs,

from ESMA, which is a good solution in comparison to the idea of EU to assigned the direct supervision of all CASPs by ESMA. This current (*ex ante*) supervision is therefore already carried out in the licensing proces [Srokosz 2025: 65-78]. Furthermore, the other provisions of the MiCAR relating to the supervision of CASPs can be grouped into two main principles, the first being the disclosure requirements imposed on CASPs and the second being a substantial set of obligations relating to the internal management of CASPs. Compliance with both requirements is subject to supervision at national and EU level. The basic instruments of *ex post* supervision include the withdrawal of authorisation for CASPs. To illustrate the links between MiCA and AML, it is worth noting that one of the legal grounds for withdrawal is a CASP's breach of national provisions transposing Directive 2015/849 (AML) (Article 64(2)(a) MiCA). Other supervisory and disciplinary measures for CASPs include: objecting to a planned acquisition of a CASPs (Article 83 MiCA), direct supervision of significant CASPs by the EU supervisor, and classic repressive and investigative supervisory measures (Article 94 MiCA) or intervention powers (Articles 103-105 MiCA), as well as the application of administrative and financial penalties (Article 111 MiCA).

The supervisory analysis must also cover the regulations resulting from the DORAR. Pursuant to Article 2(1)(f) of the DORAR, CASPs, as 'financial entities', have rightly been covered by the regulations (largely supervisory and related to reporting obligations) set out in the DORAR. This means that CASPs must also build digital resilience based on the digital risk management requirements set out in DORAR. In particular, this requires CASPs to establish an ICT risk management framework, identify, classify and prepare appropriate documentation, and counter cyber threats in relation to ICT risks, in accordance with the principles of proportionality. CASPs manage the risk posed by ICT third-party service providers as an integral part of the ICT risk covered by their ICT risk management framework. CASPs that have entered into contractual arrangements for the use of ICT services for business purposes remain fully responsible at all times for fulfilling and complying with all obligations under the DORAR and applicable financial services regulations, in accordance with the principle of proportionality. ESAs conclude administrative cooperation agreements with the relevant authorities of third countries to enable the Lead Overseer (hereinafter LO) and its team designated for this task in a given third country to carry out inspections efficiently in that third country, whereby the DORAR specifies

the essential elements of these agreements, indicating, *inter alia*, that for effective supervision it is important to specify in the agreements, firstly, the procedures for coordinating supervisory activities in the area of monitoring risks posed by ICT third-party service providers by the relevant third-country authority; secondly, a mechanism for the transfer of all relevant information between EU supervisors and third-country supervisors; thirdly, a system for the third-country authority to notify the ESA of breaches of law by a critical ICT third-party service provider, as well as the measures and sanctions applied; fourthly, regular exchange of information on regulatory and supervisory developments in the third country with regard to the monitoring of risks posed by ICT third-party service providers in the third country (Article 36(2) of DORAR).

The solutions adopted in the DORAR are intended to facilitate and enable effective supervision of ICT third-party service providers. However, the obligation to manage risks posed by ICT third-party service providers rests with financial entities (Article 28 of DORAR), and thus in this case also with CASPs, but only with CASPs that have been 'authorised' under MiCAR, as stipulated in DORAR. At this point, two situations need to be distinguished: one where CASPs operate on the basis of authorisation and another where Article 61 MiCA applies. In the first case, CASPs must comply with DORAR rules as financial entities (Article 2(1)(f) of DORAR), and in the second case, CASPs from third countries (Article 61 of MiCAR) will not be financial entities within the meaning of DORAR.

If we are dealing with a CASPs that has been authorised to operate in the EU on the basis of a MiCAR licence, then that entity, as a financial entity within the meaning of DORAR, using the services of ICT third-party service providers, is responsible for fulfilling and complying with its obligations under DORA (Article 28 DORAR). This responsibility is expressed, *inter alia*, in a legal relationship established in accordance with the principle of proportionality through contractual arrangements for the provision of ICT services between the CASPs (financial entity) and the ICT third-party service provider. Financial entities, using a risk-based approach, determine in advance the frequency of audits and controls and the areas to be controlled at ICT third-party service providers. In essence, it can be said that financial entities assume the role of 'supervisory authorities' in DORA in terms of the normative shape and control of the performance of contractual provisions with ICT third-party

service providers. Moreover, the normative shape of these agreements has been largely determined by mandatory contractual content, either explicitly indicated in the provisions of DORA (e.g. 28(7) DORA or Article 30 DORAR) or decodable from the provisions of DORAR and MiCAR.

The legal relationship between CASPs as financial entities and ICT third-party service providers is most fully expressed in Article 30 of DORAR, which regulates the necessary key contractual provisions, minimum, specific ('at least') essential elements of agreements between financial entities and ICT third-party service providers. This essential content of the contractual provisions is intended to guarantee the secure and effective supervision of the cooperation between CASPs and ICT third-party service providers. Of particular note in these provisions is the solution whereby it is possible to determine the admissibility of subcontracting by external ICT providers performing essential or critical functions for CASPs, while at the same time specifying the right of access, control and audit by the financial entity or a designated third party or competent authority.

With regard to a critical ICT third-party service provider that would be of crucial importance to a financial entity, EU supervisory authorities make this designation under the conditions and within the framework of Article 31(1) of DORAR, whereby financial entities may use the services of ICT third-party service providers established in a third country and designated as critical if those ICT third-party service providers have established a subsidiary in the EU within 12 months of the designation (Article 31(12) of DORAR). The EU competent supervisors also designate as the lead supervisory authority for each critical ICT third-party service provider the EU supervisor that is responsible for the financial entities that together account for the largest share of the total assets of all financial entities using the services of that critical ICT third-party service provider, shown as the sum of the individual balance sheets of those financial entities.

In turn, the LO designated in accordance with Article 31(1)(b) of DORAR shall supervise the critical ICT third-party service providers assigned to it and shall be the main point of contact for those critical ICT third-party service providers for all supervisory matters. The LO shall assess whether each critical ICT third-party service provider has adopted comprehensive, robust and effective policies, procedures, mechanisms and arrangements

for managing the ICT-related risks that the provider may pose to financial entities.

The competences of the LO can be classified as supervisory powers in the strict sense, as it may, inter alia: request ICT third-party service providers to provide all relevant information and documents; conduct general investigations and inspections; issue recommendations, in particular those relating to further subcontracting to ICT third-party service providers from third countries or to refrain from entering into a further subcontracting agreement, if, in the opinion of the authority, this would pose a risk to the provision of services by the financial entity or a risk to financial stability, or impose financial penalties on ICT third-party service providers. In accordance with the principle of transparency at EU level, the list of critical ICT third-party service providers is updated annually.

In particular, CASPs, as a financial entity, is responsible for ensuring, when using ICT third-party services, that the concentration risk is properly assessed so as not to become dependent on ICT third-party service providers (Article 29 of DORAR). It is worth noting that further subcontracting of ICT third-party services is not prohibited in DORAR; the regulation only states that "where the contractual arrangements on the use of ICT services supporting critical or important functions include the possibility that an ICT third-party service provider further subcontracts ICT services supporting a critical or important function to other ICT third-party service providers, financial entities shall weigh benefits and risks that may arise in connection with such subcontracting, in particular in the case of an ICT subcontractor established in a third-country" (Article 29(2) of DORAR). CASPs should also consider whether EU data protection rules are complied with and effectively enforced in that third country. Of particular importance and caution (from a risk perspective) as well as stability and secure functioning of the CA market, CASPs may find the provision that they are the ones to assess whether and how potentially long or complex subcontracting chains may affect their ability to fully monitor the functions covered by the contract and the ability of the competent authority to effectively supervise the financial entity in this regard (Article 29 DORAR *in fine*).

The efficiency and effectiveness of the exercise of the LO powers over critical ICT third-party service providers (if the supervisory objectives cannot be achieved through contacts with the subsidiary) depends, however,

primarily on the conclusion and implementation of administrative cooperation agreements by the ESAs with the relevant third-country authorities to enable, where necessary, the efficient conduct of inspections in a given third country by the LO and its team designated for that task in that third country (Article 36 DORAR).

These cooperation agreements do not create legal obligations for the EU and its Member States, nor do they prevent Member States and their competent authorities from concluding bilateral or multilateral agreements with those third countries and their relevant authorities. However, the enforcement of these provisions is subject to the consent of the critical ICT third-party service provider to carry out inspections in the third country and to the absence of any objection by the supervisory authority of the third country. Cooperation between these authorities is therefore a guarantee of effective enforcement of supervisory provisions. It is worth adding that the LO may also issue a decision (pursuant to Article 37 DORAR) requiring critical ICT third-party service providers to provide information, such as documents, audit reports, ICT incident reports or contracts necessary for the performance of supervisory duties, and any other information on parties to whom the critical ICT third-party service provider has outsourced functions or operational activities. The LO shall immediately forward a copy of the decision requesting the provision of information to the competent authorities of the financial entities that use the services of the critical ICT third-party service providers concerned and to the Joint Overseer Network.

The critical ICT third-party service provider remains fully liable if the information provided is incomplete, untrue or misleading. Another possibility to enforce the required behaviour from critical ICT third-party service providers is the institution of general investigations (Article 38 of DORAR).

The LO may conduct investigations into critical ICT third-party service providers, including: access to documents, requests for written and oral explanations from representatives of critical ICT third-party service providers, and requests for records of telephone calls and data traffic. Failure to respect these powers of the LO may result in the imposition of periodic penalty payments. The LO shall inform the competent authorities of the financial entities that use the services of a given critical ICT third-party service provider about the planned investigation and the identity of the authorised persons.

In addition, the LO also has the possibility to carry out on-site inspections, including at business premises and remotely at ICT third-party service providers. Such inspections may cover the full range of relevant ICT systems, networks, equipment, information and data used to provide ICT services to financial entities or affecting the provision of such services. Of course, the LO shall, in good time before the inspection, inform the competent authorities of the financial entities that use the services of the ICT third-party service provider concerned. The critical ICT third-party service provider shall be subject to the on-site inspections specified in the decision of the LO. This decision specifies the subject matter and purpose of the inspection, its start date and periodic penalty payments. The effectiveness of this supervisory instrument will be determined by the solution provided for in Article 39(7) of DORAR, according to which, if the officials of the LO find that a critical ICT third-party service provider opposes such an inspection, the LO shall inform critical ICT third-party service provider of the consequences of such opposition, including the possibility that the competent authorities may require financial entities to terminate their contractual relationships with that critical ICT third-party service provider³.

This is an interesting example of supervisory provisions ‘encroaching’ on civil law and previously concluded agreements between a financial entity and ICT third-party service providers, but it should be emphasised that this encroachment is justified and necessary.

Essentially, therefore, a specific ‘threat’ for critical ICT third-party service providers is the risk of a financial institution ‘terminating’ the contract under pressure from the supervisory authority to end legal relations with the critical ICT third-party service provider.

The effectiveness of supervision over critical ICT third-party service providers may also be enhanced by follow-up measures (Article 42 of DORAR) addressed both to critical ICT third-party service providers (e.g. publication of information on non-compliance or lack of information on compliance with the recommendations of the LO) and to financial entities cooperating with critical ICT third-party service providers (the supervisory authority ordering them, as a last resort, to temporarily suspend, in whole or in part, the use of the service provided by a critical ICT third-party service provider, or to terminate the relevant contractual provisions concluded with that

³ Emphasis – MF.

critical ICT third-party service provider). This ultimate supervisory measure of suspending or terminating contracts with an critical ICT third-party service provider (Article 42(6) of DORAR) already constitutes a very real ‘power’ of supervisory influence over critical ICT third-party service providers.

4. Provision of crypto-asset services at the exclusive initiative of the client pursuant to Article 61 MiCA (reverse solicitation)

A special case of CA service provision is the provision of services at the exclusive initiative of the customer. This specific nature stems from the fact that, as a rule, the provision of CA services in the EU requires authorisation. However, the regulatory framework of Article 61 MiCAR allows third-country providers to provide CA services to customers in the EU without the need to obtain authorisation.

The condition for the correct application of this provision is that, in short, the ‘EU client’ initiates, on its own exclusive initiative, the provision of CA services or the conduct of CA activities by a third-country firm. Article 61 of MiCAR is clarified by the ESMA guidelines of 26 February 2025 [ESMA35-1872330276-2030], which are in fact crucial for detecting and preventing practices, which are in breach of the provisions of Article 61 MiCAR. The objectives of these guidelines are to establish consistent, efficient and effective supervisory practices within the ESFS and to ensure the common, uniform and consistent application of the provisions in Article 61 of MiCAR. It is not the optimal solution, however, that these matters were included in *soft law* rather than in the more substantial content of the MiCAR or BTS, as they are fundamental to customer protection in the CA market with regard to the provision of services or activities undertaken by companies from third countries at the exclusive initiative of the client.

An analysis of the provisions of these guidelines reveals that the main pillars of this protection are the following rules: firstly, the rule according to which the provision of CA services following the acquisition on behalf of a third-country firm by a person or entity regulated in the EU should still be considered a violation of the MiCAR. This applies in particular to any advertising activities carried out by EU credit institutions or investment firms, even if the third-country firm belongs to the same group (point 22 of the guidelines). ESMA guidelines 26/02/2025 to Article 61 of MiCAR provide an explanation of the term solicitation by CASPs providers from

third countries. This term covers acquisition by a company, its employees, outsourcers or even influencers. The condition for classifying an activity as acquisition is acting on behalf of the company or having close ties to the company, for which the legal basis may be a contract or informal agreement and, in principle, the existence of any monetary or non-monetary benefit associated with the acquisition activity. National competent authorities should consider all the facts and circumstances of the case to assess whether a third-country firm is soliciting clients established or located in the EU.

The second important rule interpreted from the guidelines concerns the concept of exclusive customer initiative. This notion should be interpreted narrowly and reconstructed on the basis of factual circumstances. These circumstances essentially determine whether a third-country firm may provide CA services to a client without obtaining authorisation from national or EU authorities. The implementation of this rule, and thus the effectiveness of client protection, is solely linked to the need to keep records that allow the relationship with the client to be traced, and in particular whether the client took the initiative.

The third and most important rule resulting from the guidelines, as it ensures effective customer protection, is to ensure and apply adequate supervisory practices in this area, which seems to be a particularly difficult task due to the need for ongoing monitoring of the activities of third-country companies, mainly on the Internet (especially on social media and influencer media) by supervisory authorities. The effectiveness of these activities seems to depend primarily on cooperation between supervisory authorities and tax, police or AML authorities in EU countries and third countries.

The categorisation of CA and CA services or activities used by a third-country firm should be sufficiently detailed to prevent the use of the exemption for reverse solicitation to circumvent the authorisation requirement under Article 59 of MiCAR. This gives rise to specific supervisory tasks in terms of monitoring the activities of online CASPs from third countries and assessing (based on facts rather than contractual arrangements or disclaimers) whether the CASPs provider has solicited the customer or whether the contact was initiated exclusively by the customer. Of course, the institution of reverse solicitation is not new in financial market law; it also operates in the capital market (based on the provisions of MiFID II). However, it is worth noting that the CAM is more decentralised than the capital segment, and customer

protection regulation in this market appears to be weaker than in the capital market⁴.

The manner of regulation in Article 61 MiCAR raises a number of critical comments, and compliance with the boundary conditions of Article 61 MiCAR is highly illusory. On the one hand, the EU legislator's determination for a flexible approach to this article and to ensure that customers can use CA services from third countries is understandable, especially in the era of online services and the latest technologies. On the other hand, however, a reading of the guidelines highlights the challenges facing supervisory authorities and others in the process of protecting CAM customers who use the services of third countries. From this perspective, the question remains open as to whether it is appropriate to supplement the normative content of Article 61(3) MiCAR not with guidelines (as is currently the case) but with BTSs. This would result in an increase in regulation, but in such an important segment as customer protection in the CAM, it seems worth considering. While the need to ensure competitiveness in the CAM and to allow customers to decide whether to use third-party products and services in framework of inbound marketing is understandable, it should be noted that the institution of reverse solicitation in the CAM requires a special supervisory approach from the perspective of customer protection. The provisions of reverse solicitation should be subject to narrow interpretation. The burden of proof lies here with the third party. It must rigorously document that it was the customer who initiated contact. The tasks and challenges for supervisors relating to reverse solicitation must be considered particularly important in view of the weaker protection of customers in this market.

5. The outsourcing in the CA market

Due to reduced customer protection compared to other financial market sectors, the institution of outsourcing under Article 73 of MiCAR also deserves comment and attention from a consumer perspective. This raises the question of the limits of creating outsourcing chains, which is important both from the perspective of CAM customers and the financial stability of this market.

⁴ The issue of reverse solicitation in other segments of the financial market, e.g. in the payment services market or in online payments, is beyond the scope of this study. For more on this topic, see: [Mostowik 2022: 99-113].

The regulatory framework for outsourcing institutions in the CAM appears to be clear. Pursuant to Article 73 of MiCAR, CASPs who outsource services or activities to third parties for the purpose of performing operational functions are required to take all reasonable measures to avoid additional operational risk. Furthermore, they are fully responsible for fulfilling their obligations and are required to ensure, among other things, that: firstly, outsourcing does not lead to the transfer of responsibility from CASPs; secondly, that outsourcing does not alter the relationship between CASPs and their customers or the obligations of CASPs towards their customers; thirdly, outsourcing does not alter the conditions for granting authorisation to CASPs or, for example fourthly, outsourcing does not prevent the competent authorities from exercising their supervisory functions.

CASPs has rightly imposed an obligation to have an outsourcing policy covering contingency plans and exit strategies. In addition, CASPs are required to specify in a written contract their rights and obligations and the rights and obligations of third parties to whom they outsource services or activities. Outsourcing contracts give CASPs the right to terminate them. CASPs and third parties are required to provide the competent authorities and other relevant authorities, upon request, with all information necessary to enable those authorities to assess the compliance of outsourced activities with MiCAR.

The outsourcing solutions presented in MiCAR therefore provide a framework for outsourcing regulation, which establishes rules for a proper and, in the opinion of the EU legislator, secure outsourcing policy in MiCAR. Firstly, these include, above all, the rule, or even the principle (in the light of which the provisions of Article 73 MiCAR should be interpreted and explained), that responsibility for the outsourcer's activities rests with the CASPs, and this rule constitutes a specific non-transferable provision in this regulation.

This means that any contractual provisions modifying the above rules should be considered non-binding and inconsistent with Article 73 of MiCA. Secondly, it can be pointed out that outsourcing activities must not harm the customer of the CASPs. The third rule related to the boundaries of outsourcing is that any contractual provisions between providers and outsourcers cannot *de facto* change or modify the terms of the authorisation already granted to providers. And the fourth rule, which can be reconstructed from Article 73 MiCAR, concerns supervisory issues, imposing obligations on both parties to

the outsourcing relationship (providers and outsourcers) to enable supervisory authorities to carry out effective controls. It is precisely for reasons related to the need to ensure effective control and supervision that a restrictive interpretation of Article 73 MiCAR with regard to sub-outsourcing should be advocated.

6. Conclusion

Undoubtedly, the supervisory authorities are responsible for ensuring digital resilience, even though the legal framework for resilience obviously provides for a three-stage system: the internal policies and systems of a financial entity (1) supervised by a national supervisory authority (2), followed by EU supervisory authorities (3) and their normative patterns. It is the national supervisory authorities that have effective instruments at their disposal to suspend CA or ICT services and to oblige the termination of dangerous contracts with critical ICT third-party service providers. However, given the national supervisory objectives in the financial market, it is impossible to imagine any supervisory authority other than (in Poland) the Polish Financial Supervision Authority (KNF). The voices appearing in Poland in the public debate about the need to place the CAM under the supervision of an entity other than the KNF would not only undermine the objectives of financial market supervision, but would also have a negative impact on the emerging model of customer protection in this financial market, which is weaker than in other market segments due to the existence of significant and new risks in this market, including in particular the risk of speculation and the possibility of an increased risk of money laundering. Another regulatory national challenge in Poland is related to the catalogue of banking operations listed in Article 5(2) of the Banking Law in order to enable banks to apply the MiCA Regulation in full [Srokosz 2026: 19-32].

An unquestionable challenge for supervisory authorities at the national level – the KNF – should be to strike a balance between ensuring innovation in the financial market on the one hand, and proportionate but decisive supervisory measures on the other, including in particular measures to protect customers and the market as a whole. It seems that supervisors must pay particular attention to the supervisory challenges covered by the provisions of Article 36 of DORAR, concerning the exercise of supervisory powers outside the EU.

Regulatory gaps in both DORAR and MiCAR are noticeable in the area of customer protection in the CAM, especially with regard to for example reverse solicitation. The use of *soft law* to clarify or supplement this protection, which is enshrined in Article 61 of the MiCAR, also raises doubts. It seems reasonable to consider regulatory modifications in this area and to standardise customer protection in this area by means of binding legal norms, in this case: BTSs, given the specific nature of this market, its decentralisation and lack of guarantee funds, as well as the difficulties in pursuing claims by customers whose rights have been infringed.

Certain regulatory dangers and risks of abuse can also be diagnosed on the basis of Article 71 MiCAR, as well as Article 61 MiCAR in conjunction with Article 71 MiCAR.

The regulatory differences between Articles 59 and 61 MiCAR demonstrate, as also can be seen, the disproportionate nature of the solutions, creating potential scope for abuse and distortion in the application of Article 59 MiCAR. The supervisory guidelines adopted for Article 61 MiCAR without the strong involvement of financial market protection authorities may prove illusory. Of course, the scale of regulatory difficulties in the CAM is different from other market segments, given the far-reaching decentralisation of this market and its digital format. Nevertheless, or perhaps precisely because of this, it would be worth reconsidering the methods and instruments used to supervise the protection of the EU financial market and its customers. The normative concept of the EC to assign to ESMA the direct supervision of all CASPs will not – in my opinion – strengthen supervision *per se*.

There appears to be a lack of unquestionable solutions in this regard in the guidelines of 25/02/2025, as well as a lack of transparent indications as to the level of the outsourcer chain. Again, it seems that this could be too far-reaching an interference in the CAM, but in view of the somewhat flawed Article 61 of MiCAR and the associated risks for customers – including those of a procedural nature and those related to the collection of information by EU supervisory, police, AML or tax authorities – it does not seem to be merely a subject of theoretical academic reflection.

It can, of course, be argued that CAM customers have the right to make risky investment decisions as part of their general economic freedom, but it is also worth remembering that clients in this market have no guarantee funds, no

investor compensation schemes or other guaranteed benefit fund, and the existence of only a white paper and protection through information and contractual clauses may prove insufficient and cause macroprudential problems.

MiCAR and DORAR have their drawbacks and dangerous imperfections, which were discussed in this study. Ensuring the effectiveness of these two flagship regulations for the CAM rests primarily with national supervisory authorities, which are responsible for ensuring that CASPs and outsourcing agreements are properly structured through control and supervisory measures. The tasks and competences of supervisory authorities analysed in this study are justified and proportionate in their interference with the content of CASPs or outsourcer contractual provisions and are further evidence that in the era of globalisation and digital transformation of financial market law, interference from public and private law regulations is necessary to ensure financial stability and security in the CAM, protecting in this hybrid way the CAM customer, who here – due to the lack of guarantee systems – should be subject to stricter protection. Stability and security in the CAM are largely a result of the proper exercise of their powers by supervisory authorities and ensuring the necessary competitiveness on the CAM should not be at the expense of protecting customers on this market.

References

Asschemann, A.: Crypto-assets under MiCAR: a deep dive into risks, solutions, and regulatory convergence, ERA Forum vol. 24, 2023.

Buttigieg, C.P.: MiCA and the flawed premise of the centralised supervision: operational burden vs. supervisory consistency, ERA Forum vol. 27, 2026.

Buttigieg, C. P.: Preserving national supervision of CASPs under MiCAR, ERA Forum, vol. 26, 2025.

Buttigieg, C.P., Cuyle, S.: Six years of regulation and supervision of crypto-assets in Malta: The approach and lessons learned, Journal of Financial Compliance, no. 3, vol. 8, 2024.

Fedorowicz, M.: Fundusze gwarancyjne na rynku finansowym jako instrumenty przeciwdziałania kryzysom finansowym a funkcje regulacyjna i ochronna państwa [Guarantee funds in the financial market as instruments for countering financial crises, and the state's regulatory and protective functions], Przegląd Prawa Publicznego [Public Law Review], no. 4, 2024.

Fedorowicz, M.: Nadzór nad rynkiem kryptoaktywów w świetle projektu rozporządzenia MiCA- najnowsze wyzwania i tendencje regulacyjne cyfrowej stabilności i odpowiedzialności na rynku finansowym UE [Supervision of the crypto-asset market in light of the MiCAR draft – the latest regulatory challenges and trends regarding digital stability and accountability in the EU financial market, [in:] *Inwestycje alternatywne- nowe spojrzenie* [Alternative investments – a new perspective], eds. K. Królik-Kořtunik, I. Skibińska-Fabrowska, Warszawa 2021.

Fedorowicz, M.: Zasada stabilności finansowej w świetle rozporządzenia w sprawie rynku kryptoaktywów [The principle of financial stability in the context of the Crypto-Assets Market Regulation], *Przegląd Prawa i Administracji Uniwersytetu Wrocławskiego* [Journal of Law and Administration, University of Wrocław], no. 140, 2025.

Mostowik, M.: Świadczenie usług w modelu reverse solicitation na rynku płatności internetowych [Provision of services under the reverse solicitation model in the online payments market], *Monitor Prawa Bankowego* [Banking Law Monitor], no. 7/8, 2022.

Srokosz, W.: *Zakres przedmiotowy stosowania rozporządzenia MiCA: wybrane problemy* [The material scope of the MiCA Regulation: selected issues], [in:] *Księga Zjazdu Katedr i Zakładów Prawa Finansowego i Prawa Podatkowego "Misja prawa finansowego – wyzwania współczesności"* [Book of the Congress of Departments and Institutes of Financial Law and Tax Law "The Mission of Financial Law – Contemporary Challenges], eds. E. Feret, P. Majka, Rzeszów 2023.

Srokosz, W.: *Reglamentacja świadczenia usług w zakresie kryptoaktywów* [Regulation of the provision of services relating to crypto-assets], *Monitor Prawa Bankowego* [Banking Law Monitor], no. 4, 2025.

Srokosz, W.: *Zmiany w katalogu czynności bankowych wprowadzone przez ustawę o rynku kryptoaktywów* [Changes to the catalogue of banking operations introduced by the Crypto-Assets Market Act], *Monitor Prawa Bankowego* [Banking Law Monitor], no. 1, 2026.

Hrabćák, L., Štrkolec, M.: EU Regulation of the Crypto-Assets Market, *Białostockie Studia Prawnicze* [Białystok Legal Studies], no. 1, 2024.

Legal Acts

Regulation (EU) 2022/2554 (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011)

Regulation (EU) 2023/1114 (Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937)

Directive (EU) 2023/2226 (Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation)

Other official documents

Guidelines on situations in which a third-country firm is deemed to solicit clients established or situated in the EU and the supervision practices to detect and prevent circumvention of the reverse solicitation exemption under the Markets in Crypto Assets Regulation (MiCA), ESMA35-1872330276-2030

Available at: https://www.esma.europa.eu/sites/default/files/2025-02/ESMA35-1872330276-2030_Guidelines_on_reverse_solicitation_under_MiCA.pdf, accessed: March 3rd, 2026.