



DARTE SERIES

Brussels 2.0

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). Over time, the series has expanded to cover not only MiCAR but also other related regulatory frameworks.

The Brussels 2.0 DARTE edition was hosted by the European Commission on March 14th, 2025, bringing together regulators, policymakers, and industry experts to engage in high-level discussions on the harmonisation of the Digital Operational Resilience Act (DORA) and European Banking Authority (EBA) Outsourcing Guidelines, the proportionality principle in regulation, and the integration of Decentralised

Finance (DeFi) within existing regulatory frameworks.

We extend our sincere gratitude to the European Commission, Project Catalyst and DLT Finance for their invaluable support in making this roundtable possible. Special thanks to Joachim Schwerin, Rabia Karaarslan Turkut, Miguel Vaz, and Anne-Grace Kleczewski for their contributions to the discussions.

This report consolidates insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participant or the respective rapporteurs.



1. Harmonisation of DORA and EBA Outsourcing Guidelines

The first topic of the Brussels roundtable, presented by Rabia Karaarslan Turkut, Information Security Officer at DLT Finance AG, focused on the regulatory overlap between the DORA, MiCAR, and EBA's Outsourcing Guidelines.

Participants discussed the compliance challenges faced by CASPs due to fragmented and overlapping obligations under these frameworks. Particularly, concerns were raised regarding subcontracting and complex provider chains, emphasizing the difficulty in ensuring compliance beyond direct contractual relationships. Additionally, the complexity of maintaining multiple outsourcing registers, as required separately by DORA, MiCAR, and the EBA guidelines, was highlighted as a key operational burden.

Regulatory Alignment Challenges:

The roundtable explored specific compliance obligations, including:

- MiCAR Article 73: Requires CASPs to maintain written outsourcing agreements and comprehensive governance structures, with detailed documentation outlined by the regulatory technical standard (RTS) in form of a commission delegated regulation (CDR) on record-keeping.
- DORA Articles 28-30: Set rigorous standards for ICT third-party risk management, mandating via the

relevant Commission Implementing Regulation on the Register of information a structured register of third-party ICT providers.

- EBA Outsourcing Guidelines (2019): Introduce tiered governance, monitoring, and due diligence obligations, explicitly differentiating between critical and non-critical outsourcing functions.

Participants highlighted ongoing uncertainty regarding the continued applicability of the 2019 EBA guidelines to MiCA-licensed CASPs. Article 73 MiCA contains an explicit provision on outsourcing for CASP and EBA announced the replacement of the 2019 guidelines by their upcoming new Guidelines on Sound Management of Third-Party Risks, which EBA had not already published by the time of this DARTE session.

Best Practices and Solutions:

Participants positively acknowledged the approach taken by the German financial supervisory authority, BaFin. It consolidated multiple reporting obligations into a single "Notification of Outsourcing," significantly reducing redundancy and compliance burdens for CASPs.

The roundtable also highlighted the European Commission's recent removal of overly extensive ICT subcontracting chain monitoring requirements initially proposed by the European Supervisory Authorities (ESA). This adjustment was

welcomed by participants as a pragmatic step toward reducing compliance complexity.

Expert Opinion on Harmonising Outsourcing Requirements under MiCA, DORA, and EBA Guidelines

The experts agreed on the following current best practices and recommendations:

- **Promote Regulatory Harmonisation Across Applicable Regulatory Frameworks:** Industry members should work with their NCAs on consistent interpretation

and application of MiCA, DORA, and (adapted) EBA Outsourcing Guidelines.

- **Adopt Unified Reporting Mechanisms:** Industry representatives should encourage their local NCAs to develop and adopt streamlined reporting systems, mirroring Germany's "Notification of Outsourcing". This will enable CASPs to efficiently satisfy multiple regulatory obligations through a single integrated reporting mechanism, significantly reducing compliance burdens and ultimately reducing the complexity arising from fragmented national practices.

Expert Opinion on Harmonisation of DORA and EBA Outsourcing Guidelines

The key recommendations from the discussion are:

- **Push for Regulatory Consistency Across Member States:** Industry representatives should request their NCAs to align on interpretation and enforcement of MiCAR, DORA, and EBA Outsourcing Guidelines uniformly across all Member States, eliminating fragmentation and enhancing regulatory predictability for CASPs.
- **Implement Unified Reporting Systems:** Industry representatives should request to apply integrated reporting solutions comparable to German BaFin's "Notification of Outsourcing," allowing CASPs to fulfill multiple regulatory requirements simultaneously, thereby significantly reducing administrative burdens and compliance complexity.
- **Waiving outdated EBA Guidelines:** Industry associations should call for an explicit waiver of the application of the current 2019 EBA Guidelines and for promptly finalizing the new EBA Guidelines on Sound Management of Third-Party Risks, explicitly outlining their applicability to MiCA-licensed CASPs.

2. Proportionality Principle

The second topic of the Brussels roundtable, presented by Miguel Vaz, focused on applying the proportionality principle within the context of DORA and its interaction with MiCAR, particularly concerning CASPs.

Participants discussed how DORA imposes comprehensive operational resilience requirements on CASPs, irrespective of their size, significantly increasing compliance costs. CASPs are mandated to maintain robust risk assessments, implement comprehensive business continuity measures, and ensure operational safeguards for their critical or important functions. These requirements intensify the reliance on third-party ICT providers, who must also comply with stringent operational resilience, security, and incident reporting standards. The number of ICT providers offering such service is limited. The resulting compliance burdens directly increase costs for CASPs and ICT providers, impacting MiCAR's Tier 1 capital requirements. These pressures particularly affect smaller institutions, potentially leading to market concentration, reduced competition, and diminished innovation capacity.

A critical issue addressed was the complexity and rising costs associated with intra group outsourcing under DORA. Corporate groups must individually ensure compliance for both outsourcers and recipients within their structure, even when the outsourcing is internal. Financial groups may establish

dedicated ICT subsidiaries or shared-service entities which fall outside of DORA to streamline compliance, but participants agreed that these solutions could introduce additional overheads without fully mitigating costs. Streamlining intra group contracts and oversight procedures were considered beneficial, yet regulatory obligations remain demanding, especially for critical ICT functions.

Additionally, the participants addressed the importance of establishing harmonized auditing frameworks to mitigate compliance duplication. Cloud providers and ICT suppliers serving multiple institutions face redundant auditing obligations, emphasizing the need for standardized and pooled auditing approaches. Participants highlighted ongoing developments toward ISO-level auditing guidelines but stressed the urgency for more immediate practical solutions. Pooled audit models, such as those promoted by the EU Cloud User Coalition, were recognized as viable approaches to reducing regulatory burdens and compliance inefficiencies across the industry.

The experts recommended applying the proportionality principle to alleviate compliance obligations, particularly for smaller institutions. Recognizing the adequacy of existing intragroup risk management structures could significantly simplify regulatory requirements for corporate groups. Participants agreed that standardized auditing practices and collaborative audit models should be

actively encouraged by regulators and industry participants alike to streamline compliance procedures.

Expert Opinion on the Proportionality Principle

The key recommendations from the discussion are:

- **Extend Proportionality Principles to Reduce Regulatory Burdens:** Industry representatives should request their NCAs to apply proportionality and industry associations should work with regulators to include proportionality in regulatory guidelines to reduce compliance costs for smaller institutions. This will prevent a monopolisation of the market and maintain a competitive, innovative market environment.
- **Recognize Intragroup Risk Management Structures:** Company groups should discuss with their NCAs to what extent intragroup compliance frameworks could be acknowledged and industry associations should work on a proposal on acknowledging intragroup compliance structures, simplifying requirements and reducing redundant oversight obligations within corporate groups.
- **Adopt Unified and Collaborative Auditing Frameworks:** Encourage and facilitate the industry-wide adoption of standardized, pooled auditing models to minimize compliance duplication and reduce administrative burdens across the sector.

3. DeFi Integration by CASPs

The third topic of the Brussels roundtable, presented by Anne-Grace Kleczewski, explored the integration of DeFi by CASPs under DORA and its interplay with MiCAR.

Participants highlighted how the initial drafting of DORA did not fully account for developments in the Web3 market,

specifically the growing integration of DeFi protocols by centralized actors, such as CASPs, and potentially also by traditional financial institutions. A key challenge discussed was the regulatory classification of DeFi, particularly given that it cannot easily be categorized as an ICT asset or as an ICT third-party provider due to its inherently decentralized nature and lack of direct control by regulated entities. The

roundtable emphasized the need for regulatory clarity to ensure DeFi integrations are achievable without inadvertently circumventing DORA's objectives or undermining user protection.

Participants also emphasized the importance of clearly defining DeFi. A consensus emerged around distinguishing infrastructure decentralization (such as blockchain layers L1, L2, and L3) from decentralized applications built atop these infrastructures. Assessing decentralization requires specific, measurable criteria, such as the number and distribution of nodes, node clustering, centralized sequencers, or points of centralization like Infura. For decentralized applications, the existence and control of access rights, number of token holders, and their governance activity were highlighted as critical indicators.

The group considered whether regulated entities, particularly CASPs, could integrate DeFi while remaining compliant with DORA. It was broadly agreed that DeFi protocols typically do not constitute ICT assets or ICT third-party service providers under DORA due to their decentralized and community-driven governance structures. However, ambiguity persists, particularly since DORA lacks an explicit exclusion for DeFi (comparable to MiCAR's Recital 22), creating uncertainty regarding the legal permissibility of offering DeFi services in the EU.

The discussions further addressed the implications of DORA's operational resilience requirements, notably the need to mitigate service downtime and ensure reliable backup measures. Participants suggested differentiating between service downtime (manageable under regulatory oversight) and underlying infrastructure downtime (often unavoidable, similar to general internet disruptions). A practical solution discussed was for regulated entities to engage validator clusters operated by trustworthy consortiums, subject to enforceable Service Level Agreements (SLAs).

A significant point of concern was how compliance with traditional regulatory frameworks like DORA could inadvertently centralize DeFi, fundamentally altering its core decentralized nature. Participants discussed the risk that, to achieve regulatory compliance, DeFi protocols may adopt centralized features, deviating from their original ethos. They underscored the importance of developing clearly defined decentralization metrics and assessing infrastructure quality transparently, such as through structured disclosures like those promoted by initiatives such as DeFiScan.

Participants concluded that a clear regulatory taxonomy categorizing different types of DeFi integrations is essential to clarify regulatory expectations and facilitate constructive engagement between regulators and industry participants.

Expert opinion on DeFi Integration by CASPs

The key recommendations from the discussion are:

- **Establish Clear Regulatory Definitions and Taxonomy for DeFi:** Industry experts should establish precise definitions, decentralization metrics, and a clear taxonomy distinguishing between infrastructure and application-level integrations for discussion and alignment with the regulators. This would clarify compliance obligations and support innovation.
- **Differentiate Regulatory Expectations Based on Integration Type:** Develop regulatory guidance that explicitly differentiates between core regulated services, ancillary or unregulated services, and CASPs acting solely as order transmitters. This differentiation would reduce uncertainty and encourage appropriate DeFi integrations.
- **Facilitate Transparent and Collaborative Assessment of Decentralization:** Promote industry-wide adoption of structured disclosure frameworks, enabling regulators to assess DeFi protocols transparently, thus balancing regulatory oversight with DeFi's decentralized characteristics without forcing undue centralization.
- **Create Legal Certainty Regarding DeFi's Applicability under DORA:** Industry associations should work on a proposal that explicitly clarifies the extent to which DeFi is included or excluded from DORA's scope, for discussion and alignment with the regulators in order to reduce market uncertainty and ensuring DeFi protocols remain viable innovation drivers within the European financial ecosystem.

We thank all participants of the Brussels 2.0 DARTE event for contributing to the discussion:

Alessandro Darold (Kraken), Alireza Siadat (Deloitte), Ana James (XReg), Anne-Grace Kleczewski (MME), Astrid Freier (VÖB), Avtandil Papuashvili (Fung Payment, Flexicheck), Belen Suarez Lopez (Go To Innovation), Clark Povey (Zumo), Elizaveta Palaznik, Giuseppe

Maria Blasi (International Investment Bank), Hugo Volz Oliveira (New Economy Institute), James Newell (GSR), Joachim Schwerin (European Commission), Juan Ignacio Ibañez (DLT Science), Lavan Thasarathakumar (Hogan Lovells), Magnus Jones (Nordic Blockchain Association), Mariana de la Roche (BlackVogel), Mat Yarger (Demia), Miguel Vaz (Hauck Aufhäuser Digital Custody), Nina-Luisa Siedler (siedler legal), Peter Großkopf (Allunity), Peter Kerstens (European Commission), Rabia Karaarslan Turkut (DLT Finance), Sebastian Higgs (Cordial Systems), Shota Natenadze (Ripple), Thibault de Lachèze-Murel (DFNS), Thorstein Thinn, Tommaso Astazi (B4E), Walter Borst (DLT Finance).

