CYBERSECURITY AND CRYPTO-ASSETS: LEGAL PERSPECTIVES

Diana STETIU
Diana Stetiu Law Office, Bucharest, Romania
diana@web3lawyer.eu

Abstract: As crypto-assets gain popularity and economic value, their security has become a key concern for both market participants and regulators. The value of these assets is stored "on-chain," embedded in distributed ledger technology (DLT) tokens, making the security of the DLT crucial. Any vulnerabilities could lead to severe losses. To address these risks, European regulators introduced the Digital Operational Resilience Act (DORA), a significant step in strengthening cybersecurity across the financial sector, including the growing crypto market. This article describes this growing regulatory regime and advances recommendations for the sector.
Keywords: Cybersecurity, Crypto, Crypto-Assets, Crypto-Asset Service Providers, Blockchain Technology, ESMA, Markets in Crypto-Assets Regulation, Digital Operational Resilience Act, Operational Risk.

INTRODUCTION

Setting the stage

The crypto-assets market has rapidly evolved over the last decade, transitioning from a niche interest into a global financial phenomenon. This growth has sparked considerable interest from regulators, particularly as the economic value tied to crypto-assets continues to rise. Crypto-assets can be transferred and stored electronically through distributed ledger technology (DLT), such as blockchain, which underpins the integrity of digital financial systems. Crypto-assets are increasingly being integrated into financial services applications to enable near real-time transactions, accurate data recording, and more efficient payment processes.

A significant shift in the regulation of crypto-assets and related services across the European Union is approaching, with the forthcoming unification under Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023, also known as the Markets in Crypto-Assets Regulation (MiCA) (Publication Office of the European Union, 2023).

MiCA represents a significant legislative advancement by the European Union aimed at establishing a comprehensive regulatory framework for crypto-assets and their associated services. MiCA entered into force on 29 June 2023 and will become fully applicable by 30 December 2024, except for the regulation of asset-referenced tokens and electronic money tokens that started to apply already on 30 June 2024. This can be considered a landmark issue for the practice of cyber diplomacy, given the differences in preferences and crypto-assets related strategy of EU Member States who, nonetheless, have to agree on a common ruleset to govern these issues in the EU and therefore have had to negotiate and harmonise their preferences. MiCA aims for maximum harmonisation within the EU by establishing a uniform regulatory framework that applies directly in all Member States, unlike the fifth EU Money Laundering Directive, i.e. AMLD5, which led to fragmented national regulations regarding “virtual currencies” or crypto assets.

For the first time, MiCA introduces uniform rules for fungible and transferable crypto-assets that are not classified as financial instruments under MiFID II, along with issuers, offerors of such crypto-assets, and providers of crypto-asset services, ensuring maximum harmonisation across the European Union.

Building on the foundations laid by MiCA, the Digital Operational Resilience Act (DORA) introduces a new EU framework for managing information and communication technology (ICT) risks in the financial sector. DORA will apply from 17 January 2025 (Publication Office of the European Union, 2022), marking a major step forward in enhancing cybersecurity for the financial sector, including the burgeoning crypto market. While MiCA focuses on the market structure and the protection of consumers, DORA goes a step further by specifically addressing the cybersecurity challenges faced by financial entities, including those involved in crypto-assets.

In recent years, the European Union (EU) has progressively become an important player in cyber and IT security policy. This is highlighted by an ever-expanding EU cybersecurity regulatory and policy ecosystem. The EU has introduced numerous further legal acts and policies addressing cyber and IT security, particularly during the 2019-2024 European Commission (Rupp, 2024).

The Importance of Cybersecurity in Crypto

When it comes to security risks, crypto-assets and traditional financial assets share many parallels. While the mechanisms that underpin them are fundamentally different—crypto-assets rely on DLT, while cash is a physical form of value—their vulnerabilities overlap. Both crypto-assets and cash face risks like money laundering, fraud, and terrorist financing. Additionally, in both cases, the asset holder is often responsible for safeguarding their own assets, which comes with its own challenges. Individuals typically rely on intermediaries, such as banks, to safely store and manage their money. In the crypto world, where users must safeguard their private keys to access their digital assets, a similar challenge arises. Cold wallets (offline storage) offer enhanced security, but they are often cumbersome for regular transactions. To simplify this, many users rely on custodial services, such as hot wallets, which offer convenience but introduce new risks. The greater the amount of crypto-assets held by a custodian, the higher the risk becomes for the broader financial ecosystem.

Custodial wallets have, therefore, become a regulated service in the EU, permitted only to licensed entities, in order to mitigate the risks associated with holding substantial crypto-assets.

Emerging Challenges in Crypto Security

Crypto-assets bring new technical challenges that do not exist in traditional financial systems. Crypto-assets are digital tokens created with cryptography and DLT that are neither issued nor guaranteed by a central bank or public authority and can be used as a means of exchange, investment, or access to goods or services. In other words, crypto-assets can be viewed as a digitally transferable representation of a value or a right. They differ from traditional assets in that the cryptographically secured transactions that create and track crypto-assets are stored on a distributed ledger (Jaursch, 2024).

Crypto-asset owners typically store their assets in digital wallets, which function as secure storage for their private keys. Transfers of crypto-assets are conducted using asymmetric encryption, a method that involves a pair of cryptographic keys: a private key and a corresponding public key. When a transaction is initiated, the private key is used to sign the message, which can only be verified and decrypted by the matching public key. While the two keys are mathematically linked, the private key cannot be derived from the public key, ensuring security (Jaursch, 2024). In this system, the private key acts as a digital signature, confirming the authenticity of a transaction, while the public key serves as the wallet's visible address. The wallet, in essence, represents the private key's storage, identified externally by the public key. All participants in the network can trust that a transaction signed with a private key genuinely originates from the wallet associated with its public key (Jaursch, 2024).

Rather than physically storing assets like coins in a traditional wallet, a crypto wallet's balance is determined by the transaction history recorded on the distributed ledger. This ledger tracks all transactions and is used to calculate the wallet's balance at any given time (Jaursch, 2024).

If a flaw exists in the DLT infrastructure, it can potentially be exploited by bad actors, leading to widespread, irreversible damage across the network. Additionally, the immutable nature of blockchain means that once a transaction or security breach occurs, it is often impossible to reverse.

Moreover, users face heightened risks from phishing attacks, hacking attempts, and technical mishaps. If a user loses access to their private keys or falls victim to a cyber-attack, they may lose their assets permanently. This underlines the need for robust cybersecurity protocols not just for individual users but for the entire crypto market.

DORA'S ROLE IN STRENGTHENING CYBERSECURITY IN CRYPTO ECOSYSTEM

DORA's Scope

The financial sector is increasingly dependent on technology and on tech companies to deliver financial services. This makes financial entities vulnerable to cyber-attacks or incidents. (European Insurance and Occupational Pensions Authority, 2023). The growing prevalence of cyberattacks and system failures highlighted the need for a robust regulatory framework to ensure operational stability. DORA is a response to the increasing digitalisation of financial services, which, while fostering innovation and efficiency, has also heightened the sector's vulnerability to cybersecurity threats. DORA seeks to address these challenges by modernising and standardising ICT security measures across the European Union. Its goal is to create a unified, resilient cybersecurity framework that strengthens the protection and operational resilience of financial institutions across the EU.

DORA has an extensive scope, covering a wide range of financial entities across the European Union, applying to credit institutions, payment and e-money institutions, investment firms, and crypto-asset service providers (CASPs) authorised under MiCA.It also encompasses issuers of asset-referenced tokens (ARTs), central securities depositories, central counterparties, trading venues, trade repositories, and alternative investment fund managers. Additionally, it includes management companies, data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, occupational retirement pension institutions, credit rating agencies, audit firms, critical benchmark administrators, crowdfunding service providers, and securitisation repositories. Importantly, DORA will also extend to third-

party ICT service providers, emphasising its comprehensive reach across the financial and technology sectors.

DORA is designed to complement other regulatory frameworks, such as the NIS2 Directive and guidelines issued by the European Banking Authority. It ensures that the regulatory landscape remains cohesive while introducing specific measures for CASPs and other financial entities.

DORA's Impact on the Crypto Market

For CASPs, which include entities such as custodial wallets, exchanges and other trading platforms, placing of crypto-assets, providing advice on crypto-assets, and crypto-assets portfolio management, DORA introduces stringent compliance requirements. DORA provides for mandatory obligations to protect users' assets and personal data. Custodial wallet providers, for instance, must implement strong security measures to safeguard private keys and prevent unauthorised access. Additionally, exchanges and trading platforms are required to ensure that their infrastructure is resilient to cyber-attacks, thereby reducing the risk of large-scale asset losses due to hacking incidents. CASPs will need to create robust frameworks for managing ICT risks and ensuring continuity during cyber incidents. For instance, CASPs must document and manage ICT incidents, implement continuity plans, and provide cybersecurity training to their employees. A CASP seeking authorisation with a Member State regulatory and supervisory authority must provide for authorisation purposes a description of conducted audits of the ICT systems including used DLT infrastructure and security arrangements. If the CASP uses and/or develops smart-contracts, a cybersecurity source code review of them is required. A CASP seeking authorisation with a Member State regulatory and supervisory authority will need to conduct penetration tests on the ICT assets supporting critical and important functions as defined in Article 3(22) of DORA, in accordance with all the following audit test approaches: (i) black box phase (when the auditor has no information other than the IP addresses and URLs associated with the audited target), (ii) grey box phase (when auditors have the knowledge of a standard user of the information system (legitimate authentication, "standard" workstation, etc.), and (iii) white box phase (when auditors have as much technical information as possible regarding architecture, source code, telephone contacts, identifiers, etc.) before starting the analysis (European Securities and Markets Authority, 2024a).

Issuers of ARTs will also need to comply with DORA. Since these tokens are often used as a medium of exchange or store of value, ensuring their security is critical to maintaining trust in the broader crypto ecosystem. ARTs issuers must establish robust ICT risk management practices and undergo regular testing to ensure that their systems are secure. An asset-referenced token is a specific type of crypto-asset designed to maintain a stable value by referencing other assets. One could define ARTs as a subclass of stablecoins, which are designed to provide a more stable alternative to highly volatile cryptocurrencies such as Bitcoin and Ethereum. Unlike most cryptocurrencies, which derive their value purely from market demand, asset-referenced tokens attempt to maintain stability by being pegged to the value of another asset or a basket of assets. This could include fiat currencies like the U.S. dollar, commodities like gold, real estate, or even other financial instruments and crypto-assets. By linking their value to stable, real-world assets, ARTs aim to reduce the price volatility that typically characterises the crypto market.

The most well-known examples of stablecoins that function as asset-referenced tokens include Tether (USDT), which is pegged to the U.S. dollar, and Paxos Gold (PAXG), which is backed

by gold. While these are among the most prominent, the concept of ARTs can be extended to more complex tokens that reference combinations of different asset types, providing even greater flexibility for users and investors.

As regulatory frameworks like DORA come into effect, ARTs are positioned to play a significant role in the evolving landscape of digital finance.

ICT Risk Management and Internal Governance Structures

DORA sets comprehensive ICT risk management and internal governance requirements for CASPs. These requirements highlight the importance of establishing robust frameworks and controls to ensure the proper management of ICT risks.

CASPs must create internal governance structures where the management body takes responsibility for overseeing the ICT risk management framework. This involves defining, approving, and regularly monitoring the ICT governance structure, including managing risks associated with third-party ICT service providers while maintaining proper documentation.

To comply with DORA, CASPs are required to implement comprehensive ICT risk management frameworks that encompass strategies, policies, procedures, and tools. These frameworks must be regularly updated, and CASPs are expected to audit and review their systems frequently to identify and mitigate ICT risks, especially those emerging from interconnected systems. DORA prescribes specific measures to help CASPs protect against, detect, respond to, and recover from ICT-related risks.

Additionally, CASPs must establish a dedicated ICT business continuity policy with a particular focus on critical functions outsourced to third-party ICT providers. The policy must include mandatory business impact analyses to prepare CASPs for crisis management when necessary. CASPs are also required to maintain strong backup policies, recovery methods, and systems to monitor the effectiveness of their ICT resilience strategies. This includes the establishment of a learning framework to gather and analyse information on vulnerabilities and cyber threats.

To ensure preparedness in handling the evolving cybersecurity landscape, DORA mandates regular digital operational resilience training for both staff and management.

Incident Management and Reporting

DORA mandates that CASPs establish comprehensive processes for managing and classifying ICT-related incidents. This entails not only the detection, response, and management of such incidents but also the systematic documentation and reporting of these events to relevant authorities. CASPs are required to adhere to specific criteria, as outlined in secondary legislation, to classify incidents and assess their impact on operations and security. Key factors to consider include the incident's severity, the number of affected users, potential data breaches, and the broader implications for market stability.

In cases of major incidents, CASPs must ensure timely reporting to competent authorities, providing all necessary details regarding the cause, resolution efforts, and preventive measures. While CASPs can engage third-party providers to assist with reporting processes, they retain ultimate accountability for ensuring that reports are accurate, complete, and in full compliance with regulatory requirements. Failure to do so may result in penalties or enforcement actions.

Furthermore, CASPs must implement robust post-incident reviews, allowing them to identify vulnerabilities, improve response strategies, and bolster their overall resilience against future ICT threats. These reviews should be integrated into their broader risk management and business continuity plans to continually enhance incident management capabilities.

In July 2024, the three European Supervisory Authorities (European Banking Authority - EBA, the European Insurance and Occupational Pensions Authority - EIOPA and the European Securities and Markets Authority – ESMA, collectively the "ESA") published the second batch of policy products under DORA. This batch consists of four final draft regulatory technical standards, one set of Implementing Technical Standards and two guidelines, all of which aim at enhancing the digital operational resilience of the EU's financial sector. The package focuses on the reporting framework for ICT-related incidents (reporting clarity, templates) and threat-led penetration testing while also introducing some requirements on the design of the oversight framework, which enhances the digital operational resilience of the EU financial sector, thus also ensuring continuous and uninterrupted provision of financial services to customers and safety of their data (European Securities and Markets Authority, 2024c). Regarding this second batch of policy products under DORA, the ESA received, during the consultation period, more than 364 responses from market participants (265 for the technical standards and 99 for the two guidelines), including a joint response from ESA's stakeholder groups (ESMA, 2024g). All these public consultations led to specific changes to the technical standards, ensuring simplification and streamlining of the requirements, greater proportionality and addressing sector-specific concerns. ESA have consulted with the European Central Bank (ECB) and European Union Agency for Cybersecurity (ENISA) for the technical standards relating to incident reporting. (European Securities and Markets Authority, 2024e).

Resilience Testing

Under DORA, CASPs are required to implement a comprehensive digital operational resilience testing program aimed at ensuring the robustness of their ICT systems. This program must include a range of assessments, tests, methodologies, and practices focused on identifying vulnerabilities and weaknesses within their infrastructure and enhancing preparedness for cyber threats, system failures, and operational disruptions.

Routine testing for all CASPs should simulate various scenarios, from technical failures to sophisticated cyberattacks, including stress tests under extreme conditions to assess their capacity to withstand disruptions. These tests should cover key aspects such as network security, data integrity, system recovery, and the security of communication channels, particularly those essential for critical functions and transactions.

For larger, "significant" CASPs—entities playing a crucial role in the digital asset market—DORA imposes more stringent requirements. These entities must conduct advanced resilience tests, including threat-led penetration testing, at least every three years. These penetration tests are highly realistic simulations of cyberattacks executed by ethical hackers who attempt to exploit vulnerabilities in the CASP's ICT systems. By replicating the tactics, techniques, and procedures used by cybercriminals, these tests provide valuable insights into the CASP's resilience against complex and evolving threats.

Resilience testing programs must also be adaptive, evolving alongside emerging threats and technological advancements. CASPs are expected to document the outcomes of these tests

and use the findings to continuously update their ICT risk management and incident response strategies. This dynamic approach ensures that any vulnerabilities are swiftly addressed, and the resilience framework remains current with the ever-changing cybersecurity landscape.

Furthermore, testing must involve close coordination with third-party ICT service providers, as CASPs often rely on outsourced services for critical operations. By including these external partners in resilience tests, CASPs can ensure that their entire operational ecosystem, including external dependencies, is equipped to withstand cyber threats and potential failures.

ICT Third-Party Risks and Contractual Arrangements

DORA mandates that CASPs only enter into contractual relationships with ICT third-party providers that meet specified security standards. These contracts must clearly define the responsibilities of the provider concerning data protection, incident response, and cybersecurity. For example, contracts should include clauses that obligate the provider to report any security breaches or system failures in a timely manner, enabling the CASP to take immediate action to mitigate the impact on its operations.

Additionally, the contracts must outline the service levels expected, such as the availability of systems, response times for incident resolution, and recovery times in the event of disruptions. These agreements ensure that CASPs maintain a clear understanding of the provider's obligations and can hold them accountable for failing to meet performance and security benchmarks.

Contracts should also include provisions for audits and performance reviews, allowing CASPs to verify that the ICT provider continues to adhere to the required security standards over time. Regular audits serve as a safeguard, ensuring that third-party providers remain compliant with regulatory expectations and can adapt to evolving threats in the cybersecurity landscape. An essential aspect of DORA's third-party risk management framework is the stipulation regarding the termination of contracts and the need for well-defined exit strategies. CASPs must have the ability to terminate contracts with ICT third-party providers if the provider fails to meet the agreed-upon security and performance standards or if there is a material risk to the CASP's operations due to the provider's shortcomings. DORA requires that CASPs include exit strategies in their third-party risk management plans, particularly for critical ICT services. These strategies must outline the steps CASPs will take to ensure business continuity if the contract with the provider is terminated or if the provider is unable to deliver its services. This might include transitioning to an alternative provider, temporarily handling services in-house, or implementing contingency plans to minimise operational disruptions.

Exit strategies are critical for mitigating risks associated with provider failures, such as data breaches, cyberattacks, or operational breakdowns. CASPs must ensure that the transition from one provider to another is seamless, preserving the integrity of their operations and safeguarding the interests of their clients.

The Implementing Technical Standards (ITS) under the first set of final draft technical standardsfirst set of final draft technical standards (ESMA, 2024f) under the DORA of 17 January 2024, establish the templates for the register of information. These ITS set out the templates to be maintained and updated by financial entities in relation to their contractual

arrangements with ICT third-party service providers. The register of information will play a crucial role in the ICT third-party risk management framework of the financial entities (European Securities and Markets Authority, 2024b).

Another significant risk DORA addresses is *concentration* risk. This occurs when a CASP relies heavily on a single or limited number of ICT third-party providers for essential services. Over-dependence on a single provider can create vulnerabilities, as any disruption in the provider's services could have a cascading effect on the CASP's operations.

To manage concentration risk, CASPs are required to regularly assess their reliance on specific providers and take steps to diversify their ICT service providers if necessary. This could involve working with multiple providers to ensure that critical services are distributed across different vendors, thereby reducing the likelihood of a single point of failure.

DORA encourages CASPs to evaluate alternative solutions as part of their third-party risk management strategy. For example, CASPs might explore backup providers or consider establishing internal capabilities for handling critical functions in the event of a third-party failure. This approach ensures that CASPs maintain operational resilience and can continue to serve their clients even if one of their ICT providers experiences a significant disruption.

In July 2024, the three European Supervisory Authorities (EBA, EIOPA and ESMA) published their joint final report on the draft Regulatory Technical Standards (RTS) specifying how to determine and assess the conditions for subcontracting ICT services that support critical or important functions under DORA. These RTS aim to enhance the digital operational resilience of the EU financial sector by strengthening the financial entities' ICT risk management over the use of subcontracting (European Securities and Markets Authority, 2024d). These RTS specify the requirements throughout the lifecycle of contractual arrangements between financial entities and ICT third-party service providers. In particular, they require financial entities to assess the risks associated with subcontracting during the precontractual phase, including the due diligence process (European Banking Authority, 2024).

Monitoring of Critical ICT Third-Party Providers

DORA introduces provisions for the oversight of critical ICT third-party providers. While most ICT providers will be subject to these designation rules, DORA does allow for certain exemptions, such as intra-group ICT services, which are not considered to pose the same external risk as independent providers. Additionally, DORA offers an alternative path to the oversight regime, enabling ICT third-party service providers to voluntarily opt-in rather than being subject only to top-down designation by regulatory authorities. This provision offers flexibility for providers who seek to demonstrate their commitment to compliance and operational resilience.

Cross-border service provision is another significant focus of DORA. Many ICT providers operate on a global scale, which can complicate regulatory oversight. To address this, DORA imposes additional scrutiny on cross-border ICT providers, particularly those operating outside the EU. Critical ICT providers from third countries must establish a subsidiary within the EU within 12 months of being designated as critical. This ensures that these providers adhere to EU regulations and remain under the direct supervision of European authorities, reducing the risks associated with offshore operations.

Information Sharing and Supervision

While DORA does not impose mandatory requirements for sharing cyber threat intelligence, it encourages financial entities, including CASPs, to voluntarily share information related to cyber risks and incidents. This includes sharing details on tactics used by attackers, indicators of compromise, and cybersecurity alerts. The goal is to foster a more collaborative approach to cyber resilience across the financial sector, enabling entities to better prepare for and respond to cyber threats by leveraging collective knowledge and experience.

DORA also grants competent authorities broad supervisory and enforcement powers to ensure compliance with its regulations. Authorities have the right to conduct investigations, inspect CASPs and their third-party providers, and access any necessary documents or data that may help assess compliance. In cases of non-compliance, penalties can be imposed, which can include fines or other sanctions, ensuring that CASPs and their ICT providers are held accountable for any failures to meet their obligations under DORA. This supervisory structure is crucial for maintaining the integrity and resilience of the financial sector's digital infrastructure.

CONCLUSION

By formally including CASPs within the regulatory concept of financial entities, DORA subjects them to the same rigorous ICT risk management and operational resilience requirements as traditional financial institutions. This represents a significant elevation in the expectations placed on CASPs, which must now meet high standards of governance, incident management, and third-party oversight to ensure the security and stability of the digital asset ecosystem.

In general, the growing importance of cybersecurity in the crypto industry cannot be overstated.

DORA's strict regulatory framework compels CASPs to adopt robust cybersecurity protocols, perform regular resilience testing, and establish comprehensive governance structures. The imposition of these requirements not only enhances the security of crypto-assets but also strengthens the overall financial system by reducing the risks of cyberattacks and operational failures. CASPs, much like banks and payment institutions, are now held accountable for ensuring the protection of both their own operations and the assets of their clients.

As the crypto market continues to expand, CASPs must rise to the challenge of aligning with DORA's high compliance standards. Failure to do so may result in significant penalties and loss of trust, highlighting the critical need for CASPs to prioritise cybersecurity as a fundamental aspect of their operations. By including CASPs within the broader financial regulatory framework, DORA reinforces the notion that digital asset providers are integral to the future of the financial system, with all the responsibilities and obligations that come with it. Cybersecurity, therefore, is no longer just a best practice for the crypto industry—it is a mandatory pillar for sustaining trust, stability, and growth in the digital financial landscape. The emerging regulatory landscape to govern these issues, which is both comprehensive and encompassing all Member States, is the result of significant cyber diplomatic efforts between Member States, EU institutions and other stakeholders such as financial institutions and crypto solutions companies.

REFERENCE LIST

Rupp, C. (2024) Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies and Actors. Berlin, Interface.

Jaursch, J. (2024) A Look Ahead at EU Digital Regulation: Oversight Structures in the Member States. Berlin, Interface.

Publication Office of the European Union. (2022) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. L333, 1-79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj [Accessed 5th September 2024]

Publication Office of the European Union. (2023) 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. Official Journal of the European Union. L150, 40-205. https://eur-lex.europa.eu/eli/reg/2023/1114/oj [Accessed 5th September 2024]

European Securities and Markets Authority. (2024a) Final report on certain technical standards under MiCA – First Package. European Union, European Securities and Markets Authority. https://www.esma.europa.eu/sites/default/files/2024-03/ESMA18-72330276-1634_Final_Report_on_certain_technical_standards_under_MiCA_First_Package.pdf [Accessed 4th September 2024]

European Securities and Markets Authority. (2024b) ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification. https://www.esma.europa.eu/press-news/esma-news/esas-publish-first-set-rules-under-dora-ict-and-third-party-risk-management [Accessed 4th September 2024].

European Securities and Markets Authority. (2024c) Spotlight on Markets - July 2024, What's Next for MiCA and DORA? https://www.esma.europa.eu/sites/default/files/2024-08/Newsletter_July_2024.pdf [Accessed 4th September 2024].

European Insurance and Occupational Pensions Authority (EIOPA). (2023) Digital Operational Resilience Act (DORA). https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en [Accessed 4th September 2024].

European Securities and Markets Authority. (2024d) ESAs published joint Final report on the draft technical standards on subcontracting under DORA. https://www.esma.europa.eu/press-news/esma-news/esas-published-joint-final-report-draft-technical-standards-subcontracting [Accessed 4th September 2024].

European Banking Authority. (2024) ESAs published joint final Report on the draft technical standards on subcontracting under DORA. https://www.eba.europa.eu/publications-and-media/press-releases/esas-published-joint-final-report-draft-technical-standards-subcontracting-under-dora [Accessed 4th September 2024].

Diana STETIU is one of the best-known fintech lawyers in Romania and internationally, recognised for her extensive experience and deep knowledge of blockchain, smart contracts, and cryptocurrency matters, including initial digital token offerings.

A law graduate of both the University of Bucharest and Paris 1 Panthéon-Sorbonne, Diana has a strong academic foundation that complements her practical expertise. By background, she is a finance and banking lawyer registered with Bucharest Bar, with over 12 years of experience representing lenders and borrowers in leveraged finance and banking transactions, as well as advising private organisations on a broad range of commercial transactions, compliance, and corporate governance matters. In 2020, Diana established her own boutique law consultancy.

Her impressive client portfolio includes technology companies, broker-dealers, major investment banks, financial institutions, asset managers, token sellers, cryptocurrency exchanges, token marketers, and venture, hedge, and private equity funds and their portfolio companies.