DIGITAL CURRENCIES
Governance Group

DIGITAL OPERATIONAL RESILIENCE ACT

DCGG POSITION PAPER

The Digital Currencies Governance Group (DCGG) welcomes the European Commission's proposal on Digital Operational Resilience (DORA). Our members concur with the principle underpinning DORA – that standardisation will drive cyber robustness in the financial services and crypto-assets sectors. Yet, just as DORA recognises that digitalisation and operational resilience are two sides of the same coin, **we recognise that regulation and innovation are two parts of the same journey towards a secure digital future**. Building cyber resilience is an inherently creative and strategic process. It involves consideration of issues such as alternative methods of service delivery and planning how to communicate in moments of crisis. **Zero-knowledge proof technology would be such an alternative solution that would improve digital operational resilience as an effective means of data transfer without jeopardising data privacy**. Therefore, we urge EU policymakers to consider **developing a proportionate, forward-looking and truly technology neutral Regulation**. As a broad principle, DCGG asks policymakers to consider **compliance requirements based on incentives, rather than penalties**. This will encourage the technology community to come up with new, more efficient ways, to reduce cybersecurity risks. Towards that aim, we would like to point to four critical areas for further consideration in DORA.

Issue I: Supervision and Harmonisation (Article 43.p.2)

Problem:

Given the cross-border nature of ICT risks, action at Member State level only has a limited effect. Furthermore, the uncoordinated national initiatives have resulted in overlaps, inconsistencies, duplicative requirements, high administrative and compliance costs - especially for cross-border financial entities

Solution:

Member States should be able to collect data; however, the bodies that are responsible for the supervision and harmonisation should be the European institutions. Thus, they can ensure that the same rules apply in all Member States. We believe that the EU should allocate supervisory powers at an ESA level instead of giving more powers to the Member States. This would create a harmonised system across the EU, that is easier to comply with.

Any information sharing between private sector participants should also be enabled through third-party intermediaries that provide a safe and trusted place for anonymous threat information to be shared which can be facilitated through technology solutions such as Zero-Knowledge Proof (ZKP) which can serve to provide access to electronic information in encrypted environments without compromising large amounts of sensitive information and data. It can be used to promote much more secure information sharing amongst the private sector.

Issue II: Regulatory Overlap

Problem:

Financial entities and crypto-asset market participants are already subjected to cybersecurity requirements in existing legislations, which poses a risk of duplication of obligations. Specifically, a harmonised system of ICT incident reporting requirement is a key provision.

However, without alignment between regulatory obligations, it might be unnecessary and impractical.

- The EU General Data Protection Regulation already requires firms to report personal data breaches.
- Financial services firms and CASPs receive many information security attacks a day; a requirement to immediately report security incidents would detract firm resources from responding to and addressing attacks or incidents.

Solution:

DORA should ensure a compatibility of requirements and a harmonised EU approach. Legislators should aim to create a Regulation that does not have too excessive standards so as not to prevent innovation. EU legislation should support innovation by creating clear and easy to follow rules and procedures and should prevent regulatory overlap which will hinder decision-making and hamper organisational performance. Consistency with international approaches is also imperative.

Issue III: ZKP & Innovation

Problem:

It is important to promote and make good use of technological solutions such as Zero-Knowledge Proof (ZKP) which allows for the secure transferring of data without compromising users' sensitive information, thus protecting their privacy and respecting legislation such as the GDPR as much as possible.

Solution:

The use of innovative solutions developed by the blockchain community such as the ZKP, has the potential to facilitate the ICT management and reporting risks processes, making them secure and cost effective. By using technologies such as ZKP we can ameliorate the significant differences that exist between the financial entities that DORA is trying to regulate, thus giving them a level playing field and providing the same level of security to their consumers. The ZKP technology allows for developing digital identification mechanisms that do not obligate users to reveal personal sensitive information which will allow the European institutions and agencies to verify the origin of the information without disclosing their source of information.

Issue IV: Proportionality

Problem:

- DCGG members are concerned about the "one-size-fits-all" approach in DORA, which will hamper innovation and flexibility.

- The EU market consists of various institutions of different sizes, types, structures, etc. Proportionality is required to ensure that any framework is flexible enough to allow for the variety of institutions across the EU.

- Additionally, crypto-asset market participants, which are in scope for DORA, should be enabled to explore how blockchain developments could improve their operational resilience – for example, by using innovative encryption approaches to further safeguard client data and assets.

- DORA requires that financial entities ICT risk management frameworks implement policies and protocols for strong authentication mechanisms, including such that prevent access to cryptographic keys and encrypted data (ZKP).

Solution:

Development of the 'proportionality' principle and proportionate application of requirements. Furthermore, DORA and its technical standards should acknowledge ZKP and innovative tech solutions as tools for in-scope entities to use as a part of their stronger ICT risk management frameworks.

Issue V: Transitional Period (Article 56)

Problem:

In its current form, DORA left the option for voting on the transitional period following which the Regulation becomes applicable.

Solution:

DCGG supports having a transitional period of 18 months following the entry into force of DORA so to allow companies to adopt the legislation and restructure in line with the new requirements.