

## CIPL Submission to the Digital Regulation Cooperation Forum (DRCF) workplan 2023 to 2024: Call for input

### I. Introduction

The Centre for Information Policy Leadership (CIPL<sup>1</sup>) welcomes the opportunity to provide input to the Digital Regulation Cooperation Forum (DRCF) workplan 2023 to 2024 by answering to the questions presented in its call.

- 1. Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits.*

### Digital Assets in blockchain

Digital assets in blockchain are transforming financial services, both traditional and new, and are taking a foothold in many forms in the an expanding digital economy. As financial services regulators seek to put their arms around this fast evolving area in the US, UK, EU and other jurisdictions, it is imperative that data privacy issues are considered and addressed in tandem with the development of financial services policy and regulation to ensure a coherent, comprehensive and workable regulatory approach, and to support an open, innovative and competitive market in the UK. This interplay is particularly important for the ecosystem in blockchain networks given the foundational role of privacy in establishing and maintaining “trust” in the myriad of financial services innovations being developed. The key elements of blockchain - transparency, immutability, borderless and de-centralised infrastructure – challenge many core concepts of privacy. This needs to be urgently addressed to enable users, providers and the technology and innovation supporting digital assets to continue to innovate with certainty, and to ensure that the UK attracts both talent and investment to be a market leading in digital assets and crypto.

---

<sup>1</sup> CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

Research published by the UK Financial Conduct Authority in 2021<sup>2</sup> estimated ownership of cryptocurrencies was up to around 2.3 million individuals globally, an increase from around 1.9 million in 2020—with 78% of adults having heard of cryptocurrencies. The total market capitalization of stablecoins has grown from \$2.6 billion at the start of 2019, to \$20 billion in September 2020—with global trading volumes estimated at \$198 billion in April 2021<sup>3</sup>.

Decentralized Finance (“DeFi”), a branch of the crypto ecosystem, accounts for a total value locked (“TVL”) in DeFi services from \$600 million in January 1st 2020 to a peak around \$315 billion in December 2021, yielding a growth of 524% in two years<sup>4</sup>. While the TVL has since dropped, it remains well above \$250 billion. In a geographical analysis of DeFi activity, Chainalysis highlights<sup>5</sup> that a large part of the DeFi growth has been driven by professional and institutional investors particularly from the European financial service sector. It is clear that the economic impact is too significant to be overlooked.

Digital assets in blockchain should be a key priority for the ICO and FCA in 2023 and 2024, and will be of interest to the CMA and Ofcom, as data and digital are core to digital assets. Clear analysis and direction of the interplay of privacy with digital assets will help ensure that the UK is a thought leader in this space, and to establish practical and proportionate approaches which support responsible innovation.

### **Privacy enhancing technologies**

Both in the context of digital assets and more broadly, Privacy enhancing technologies (PETs) can be a useful instrument to safeguard data security as well as data privacy and to bridge tensions with existing data protection frameworks. For instance, zero-knowledge proof technology can verify the authenticity of a given transaction without providing access to the underlying data and has the potential to function as a standard encryption baseline for blockchain applications. PETs have the potential to be deployed broadly and by a larger group of private and public organisations, to mitigate privacy risks, aid and streamline legal compliance and establish trust in the development and use of digital technology. PET research beyond the initial ICO draft guidance should be a further priority on the DRCF work plan, especially in the areas where the different DRCF regulatory disciplines interact and overlap with data privacy rules (e.g. online safety / content moderation and data privacy, data security and data privacy, competition and data privacy, children’s rights and data privacy).

---

<sup>2</sup> Financial Conduct Authority [Research Note: Cryptoasset consumer research 2021](#)

<sup>3</sup> TheCityUK [Cryptoassets: Shaping UK regulation for innovation and global leadership](#)

<sup>4</sup> European Commission [Decentralized Finance. Information frictions and public policies: approaching the regulation and supervision of decentralized finance](#)

<sup>5</sup> Chainalysis [The 2021 geography of cryptocurrency report: analysis of geographic trends in cryptocurrency adoption, usage and regulation](#)

## Accountability frameworks

Accountability has become a foundational stone of data privacy law, policy and best practice compliance among both private and public sector organisations. With increased regulatory expectations and the need to establish trusted and responsible data use and, many organisations have been developing privacy management programs to operationalise legal requirements, manage privacy risks and compliance and be able to demonstrate compliance and responsible use of data internally to management, to corporate boards and externally to regulators, auditors, corporate clients. CIPL has done extensive research on accountability and has published a [number of influential papers](#) on the topic.

The ICO has also emphasised the importance of accountability and has developed their Accountability Framework, to help organisations implement and measure accountability.

CIPL very much supports these initiatives. In the context of the DRCF workplan and further priorities, CIPL would like to suggest the following focus areas:

- a) a wider and more explicit recognition by all DRCF regulators of the importance of accountability in their respective regulatory competence;
- b) the development of a consensus and common cross-regulatory framework on the elements of accountability, which are risk-based, outcome based and common to all regulatory areas. CIPL works shows that accountability is law agnostic and can be applied in any area of digital regulation<sup>6</sup>. It would be desirable for companies operating in the UK to be able to work with a common framework that can leveraged across all relevant areas of digital compliance with the competence of DRCF regulators;
- c) more proactively incentivising and encouraging by providing tangible benefits for organisations that can demonstrate their digital responsibility in the given regulatory area<sup>7</sup>.

## Cross-regulatory sandboxes

CIPL has been supporting the development and wider adoption of regulatory sandboxes, as developed by the FCA, ICO and CMA. We would like to see further cross-regulatory sandbox projects launched within DRCF, especially in areas with interdisciplinary overlap and interaction – such as online safety / content moderation and data privacy, or children’s rights and data privacy, of digital assets and data privacy, or competition and data privacy.

---

<sup>6</sup> CIPL White Paper - [Organizational Accountability - Existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law](#) and CIPL White Paper - [Organizational Accountability - Past, Present and Future](#)

<sup>7</sup> CIPL White Paper - [Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions](#)

DRCF should consider proactively putting further resources into the development of such cross-regulatory sandboxes. More organisations should be incentivised to participate.

### **Transborder data flows**

Transborder data flows are one of the key areas and yet also the most complex issues of corporate compliance for both large and small organisations. Beyond just regulating the sharing of personal data through data protection laws, we see an increasing trend of data localisation requirements globally. Yet, it is essential to enable free and trusted data flows for the development and deployment of new technologies such as AI, for productivity and efficiency, to enable health and medical research and many other beneficial uses of data, that fuel economic growth and societal progress at large. The UK Government has taken steps to prioritise free, trusted and accountable data flows and has set up an Expert Council to advise on the matter.

Given that cross-border data flows are inevitable and often essential to all the regulatory domains of the DRCF, CIPL would like to suggest a cross-disciplinary project and working group to identify essential and necessary data flows in the respective areas and consider how these data flows can be enabled in compliance with the existing and, perhaps future new, rules and transfer mechanisms.

- 2. In line with the 'factors we consider when prioritising work' (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan?*

Coherence, Collaboration and Capability themes are all relevant to the intersection of digital assets and privacy. Given the unprecedented growth in this sector, and the need for both innovators and traditional financial institutions to have clarity as to how they can engage in digital assets, it is essential that privacy and financial services partner effectively in regulatory and policy development. In the fight against financial crime, we can see how the balance between requirements to know customers better and monitor financial transactions can create tensions with privacy obligations to limit data processing, particularly of special category and criminal data, and concerns about automated decision making. The UK was able to navigate these tensions through the provisions of the Data Protection Act 2018 (Schedule 1 Section 12), but they remain open issues in many other jurisdictions, leading to uncertainty and an overly cautious approaches to data processing, with the consequences that less than 1% of laundered money is ever recovered<sup>8</sup>.

As the nature of digital assets continues to grow and evolve, it is increasingly important that a coherent regulatory approach is developed. Already the Data Protection Authorities in France and Singapore, and the European Parliament and EU (e.g. Markets in crypto-assets Regulation

---

<sup>8</sup> Forbes [Why Organized Illicit Finance Demands An Organized Global Response](#)

"MiCA") are developing approaches to digital assets, some of which are helpful. If the UK wishes to support a pro-innovation economy, it also needs to be ready to tackle and provide practical policy thought leadership for digital assets on blockchain. Digital Assets are a current reality, not just a future potential, making this an urgent priority for 2023.

- 3. Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?*

Digital assets have the potential to impact all members of the public, whether through NFT's, crypto currencies, tokenisation of assets, etc. Consumers, businesses and the financial services sector itself are all impacted. A focus on vulnerable consumers and children, as digital assets are made more readily available through social media channels, is certainly a priority. The cross-border nature of digital assets also needs to be addressed.

The DRCF is encouraged to be open and consultative going forward to leverage the full breadth of business engagement and to build trust in the model.

An important element of capacity building in stakeholder engagement is the ability to rely on tools that can provide practical support for innovators and greater coherence to the regulators' work. In this sense: the development and adoption of standards and codes of conduct can ease navigation of overlapping regulations; and the simplification of the sandbox model would help decrease the necessary investment and allow start-ups and SMEs to cooperate on potentially less complex issues.

## **II. Conclusion**

CIPL is grateful for the opportunity to provide input to the DRCF workplan 2023/2024. CIPL supports DRCF's work: cooperation between regulators and business takes time and persistence, but we strongly believe it will lead to sustainable outcomes for the digital ecosystem in support of innovation.

If you would like to discuss any of the comments in this paper or require additional information, please contact Bojana Bellamy [bbellamy@huntonAK.com](mailto:bbellamy@huntonAK.com), Natascha Gerlach [NGerlach@huntonak.com](mailto:NGerlach@huntonak.com), or Camilla Ravazzolo [cravazzolo@huntonak.com](mailto:cravazzolo@huntonak.com)