CAI0072

Written evidence submitted by the Information Commissioner's Office

About the Information Commissioner's Office

The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Privacy and Electronic Regulations 2003 (PECR), the Network and Information Systems Regulations 2018 (NIS) and the Environmental Information Regulations 2004 (EIR).

The ICO is independent from government and upholds information rights in the public interest, promoting transparency and openness by public bodies and organisations and data privacy for individuals. It does this by providing guidance to individuals and organisations, solving problems where it can, and taking appropriate action where the law is broken.

Introduction

The ICO welcomes the opportunity to respond to Parliament's inquiry into the crypto-asset industry. Technology continues to develop at pace, changing how we interact with each other in digital spaces and disrupting traditional economic structures. Appropriate privacy safeguards are critical to maintaining trust in emerging technologies, including the distributed ledger technologies (DLT) that underpin the crypto-asset industry.

The ICO has responded to past developments in the crypto-assets industry[1] and is undertaking early work to assess the implications of this technology to ensure we are in a position to facilitate responsible innovation in decentralised finance (DeFi) markets. In addition to being a focus of our own foresight work, we are leading a joint examination of the regulatory risks and opportunities of Web 3.0 with the Financial Conduct Authority, supported by other Digital Regulation Cooperation Forum (DRCF) colleagues under the auspices of the DRCF Horizon-Scanning Workstream. The purpose of this work is to understand the promise and criticisms of Web 3.0 technologies, including crypto-assets such as non-fungible tokens (NFTs) and other methods of distributed exchange, allowing the UK's key digital regulators to prepare for this emerging technology if, or when, it is implemented at scale.

The application of data protection law in systems where control is both decentralised and distributed and where personal data is often permanently embedded in public transaction records, raises important issues for transparency and the exercise of information rights, among other things. This response does not communicate ICO policy with regards to crypto-assets but rather surfaces potential concerns for data protection associated with the operation of public and permissionless DLT.[2]

---

[1] In August 2019 we issued a joint statement with other data protection authorities in Australia, the EU and the USA, amongst others, in response to the proposals at that time from Facebook around their proposals to implement the Libra blockchain

[2] ICO analysis on other relevant technology, particularly Central Bank Digital Currencies, can be read in Deputy Commissioner Stephen Bonner's evidence to the Lord Economic Affairs Committee.

Controllership in decentralised structures

UK data protection law specifies that the entity responsible for exercising overall control over the purposes and means of processing personal data is the "controller". Controllers are the decision-makers, and many of the UK GDPR's obligations on transparency, lawfulness, access, security and maintaining privacy standards rest with them. However, the decentralised nature of networks common to the crypto-asset industry raise questions as to which of the many parties involved in decision-making are controllers (or joint controllers) and thus subject to particular requirements under data protection law. This forms part of a broader question about liability in decentralised structures which we understand is under active consideration by the Law Commission.[3]

This issue may be particularly acute in certain environments. For example, Decentralised Autonomous Organisations (DAO) are entities with no central governing body that use the blockchain to distribute decision-making power across token holders (i.e. users with ownership in the decentralized protocol). The operation of the DAO is written into smart contracts and token holders within the DAO vote on changes they perceive as the best interests of the organisation as a whole. Where DAO policy relating to the processing of personal data is being considered, any participating token holder could play a role in determining the purposes and means of processing.

In effect, this could create a large set of joint controllers who share accountability for their processing of personal data (the number of voting individuals in a DAO can be in the thousands or more). This can create a number of practical challenges, such as (i) ensuring that all parties understand their regulatory obligations; (ii) determining who individuals ('data subjects') may approach to exercise their information rights; and (iii) undertaking enforcement action against controllers in the event of non-compliance.

Similar issues are encountered when considering who may attract obligations as a 'processor' under UK GDPR (the entity acting on behalf of, and only on the instructions of, the relevant controller/joint controllers). Additionally, the status of operators of services utilised in the DAO (i.e. the underlying public blockchain, smart contracts or relevant cryptocurrency exchange) needs to be considered to determine what, if any, obligations those operators may have as a controller, joint controller or processor.

International data transfers

Questions of responsibility for the proper handling of personal data in a blockchain are also relevant for international data transfers. An attractive feature of decentralised structures for many individuals is its advertised inclusivity and global reach; users can ostensibly move crypto-assets wherever they want, including across jurisdictions. However, data protection law lays out the requirements to safely transfer personal data to countries outside the UK or to international organisations, with different conditions attached to those transfers if the destination is covered by 'adequacy regulations'.

[3] Calculations on identifying controllership may change when considering private, permissioned DLTs.

Where personal data is involved in transactions (i.e. wallet/transaction information relates to an identified or identifiable natural person), those responsible for processing in decentralised systems will need mechanisms to make compliant international transfers.

Transparency and re-identification of users

It is common to cite the ostensible anonymity of blockchain transactions as one of the technology's privacy strengths. Where there is true anonymity (e.g., no means reasonably likely to be used to identify an individual, directly or indirectly) the blockchain will not be processing personal data and therefore data protection legislation will not apply.[4]

While blockchain transactions may not involve certain personal data such as an individual's name, that does not itself eliminate the possibility that individuals could be identified. This is because information recorded as part of blockchain transactions may be *pseudonymised data* (and therefore still personal data) rather than anonymous information. Pseudonymised data does not directly identify individuals, but the identity of the person can be determined by using additional information.[5]

For example, information about the transactions of an user may be stored on the blockchain in hashed form (i.e. the result of converting plaintext to ciphertext). This means it is not immediately attributable to a named individual. However, the individual may still be identifiable if cryptographic protections were undermined or if they were singled out in the context of these transactions.

If it is reasonably likely that a link can be established between the information processed by a blockchain system and an identified or identifiable individual (even if the information does not enable the "real world identity" of that individual to be determined) then this information is personal data and falls under UK data protection law.

The risk of re-identification grows with the volume of data stored on the blockchain. As points of data are progressively added through additional transactions, and as DeFi payments transition to paying for real-world goods and services, an increasingly detailed view of the wallet holder can be constructed, e.g. of their personal preferences, behaviours and attitudes. The very trust mechanism for decentralised systems that requires transaction information to be permanent and public also creates significant implications for any failure of anonymity. This is a risk that operators and policymakers need to be mindful of, particularly as associative analytical tools that could establish these links grow in sophistication.

Exercising information rights

The permanent, immutable nature of storage on blockchains means that any data is retained indefinitely. In cases where personal data is on the chain (i.e. where it is reasonably likely for individuals to be identified or identifiable), the

[4] See ICO Draft Guidance on Anonymisation, Pseudonymisation and Privacy Enhancing Technologies, Chapter 1: Anonymisation.
[5] See ICO Draft Guidance on Anonymisation, Pseudonymisation and Privacy Enhancing Technologies, Chapter 3: Pseudonymisation.

permanency of data on the ledger raises potential concerns for compliance with data protection law and the exercise of individual rights such as rectification and erasure.

The UK GDPR's principle of storage limitation stipulates that personal data be retained for no longer than necessary to achieve the purposes of processing, a requirement that might be difficult to reconcile with indefinite retention on the blockchain. This same feature of blockchains may make it be difficult for an individual to exercise their right to erasure or rectification, for example in cases where inaccurate information has made it into the ledger or they want to remove their personal information from the chain. As each block in a chain contains a cryptographic hash of the previous block, any intervention to change or remove the content of a given block would disrupt the chain and undermine the trust mechanism. Storage limitation, rectification or erasure may therefore not be possible in current popular applications of the technology.[6]

Conclusion

The governance structure, transparency, permanency and immutability of DLT can present challenges to data protection. Encouragingly, industry is confronting some of these issues; firms are examining how to edit the chain or how privacy-enhancing technologies might protect against re-identification in decentralised environments, including how personal data may be processed off-chain and therefore not recorded on the ledger.[7] We encourage further exploration of these solutions as part of a data protection by design approach to the development of DLT.

The ICO is committed to helping industry, consumers and government unlock the benefits of DLT-based technology whilst ensuring the UK continues to enjoy high standards of privacy and security. Further ICO analysis on DLTs and related technologies will be forthcoming as we continue to consider the data protection implications of decentralised ecosystems.

September 2022

[6] The ICO is aware that some technical approaches are being explored that may facilitate change or erasure without corrupting the chain.

[7] See ICO Draft Guidance on Anonymisation, Pseudonymisation and Privacy Enhancing Technologies, Chapter 5: Privacy-enhancing technologies.