The Information Commissioner's response to the Bank of England and HM Treasury's consultation on a Central Bank Digital Currency (CBDC)

About the ICO

1. The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOIA), the Network and Information Systems Regulations 2018 (NIS), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR).

2. The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and it takes appropriate action when needed.

3. The Information Commissioner's Office (ICO) sets out its strategic vision in the ICO25 plan, which highlights promoting regulatory certainty, empowering responsible innovation and safeguarding the public as key priorities.[1]

Introduction

4. The ICO welcomes the opportunity to respond to the Bank of England (the Bank) and HM Treasury (HMT) consultation paper, 'The digital pound: A new form of money for households and businesses?'. The consultation assesses the case for a retail Central Bank Digital Currency (CBDC), including consideration of individuals' privacy, user control, and the proper use of personal data in line with UK data protection laws[2].

5. We recognise that this consultation paper primarily constitutes exploratory work, while a decision is reserved for a later date on the

[1] ICO25 strategic plan | ICO
[2] The digital pound: a new form of money for households and businesses? Consultation Paper (bankofengland.co.uk), p. 14.

potential introduction and specific design of a UK CBDC. As such, this response sets out our views – based on currently available information – at this stage of CBDC policy development, specifically in relation to important data protection matters that should inform future decisions on CBDC design. Key considerations include the data protection principles, requirements relating to a 'data protection by design and by default' approach, and the importance of Data Protection Impact Assessments (DPIAs).

6. We are of the view that early and continued dialogue on data protection matters can facilitate the development of a CBDC with enhanced privacy functionality and greater user control over personal data. We are committed to continuing our engagement with the Bank, HMT, and other relevant stakeholders as plans for the development of a CBDC move forward.

Key data protection and privacy considerations

7. The ICO welcomes the engagement undertaken throughout the policy development and consultation process on data protection issues. The Bank and HMT must continue to ensure policy positions on privacy and personal data processing are clear and robust so that the public and organisations have an accurate understanding of the way in which the design of a CBDC will respect people's information rights.

8. In particular, the principles set out under Article 5 of the UK GDPR should inform the policy positions and technical design[3] of any future CBDC. These principles provide an underlying framework for ensuring the personal data processing that underpins a CBDC respects individuals' information rights and limits the risk of harm. Areas for HMT, the Bank, and wider stakeholders to consider include:[4]

    - **Lawfulness, Fairness and Transparency[5]**: this principle ensures that, where personal data is being processed, it occurs in a fair and lawful way and individuals ('data subjects') are made aware of the processing that takes place. Personal data must be used in a way that is fair and those processing personal data must be clear, open and honest with people from the start about how they will use their information. Payment Interface Providers (PIPs) must ensure that the conditions under which personal data is going

[3] We note that possible privacy technology requirements of a CBDC are mapped against the data protection principles in Table B of the Bank of England Technology Working Paper.
[4] A guide to the data protection principles | ICO
[5] Principle (a): Lawfulness, fairness and transparency | ICO

to be accessed, and the way in which that data is going to be used when PIPs interact with the core ledger, are transparent and clear to individuals to support the building of public trust in a CBDC.

- **Purpose Limitation[6]:** this principle ensures organisations ('data controllers') do not reuse or repurpose personal data they have collected from individuals, without having a legitimate and lawful basis for doing so. We understand the possible use cases for a CBDC beyond standard payments (eg consent to programmable money, smart contracts, micropayments) are still under consideration. It will be crucial to ensure that the purposes of any personal data processing under potential use cases are lawful and transparent from the start of the design process. Parties processing personal data within a CBDC ecosystem must specify and record their processing purposes, so they can inform individuals in accordance with their data protection obligations.

- **Data Minimisation[7]:** this principle ensures that data controllers' collection of personal data is limited to what is necessary for delivering their product or service. The personal data PIPs will process during user onboarding and payment transactions – as well as other potentially more sophisticated data processing for use cases involving PIPs and/or the core ledger – must be adequate to properly fulfil their stated purpose, be relevant to that purpose, and be limited to what is necessary. This principle is also relevant to the building and operation of the Bank's core ledger, to the extent this involves personal data processing.

- **Accuracy[8]:** this principle means data controllers are responsible for ensuring personal data is up to date and correct. This will be an important consideration when determining what technology underpins personal data processing between PIPs and the core ledger. For example, if distributed ledger technology – which could store personal data in a manner which is permanent and immutable – is used, consideration is needed as to how people can exercise their 'right to rectification'.[9]

- **Storage Limitation[10]:** this principle means data controllers can only keep personal data for as long as it is necessary for the

[6] Principle (b): Purpose limitation | ICO
[7] Principle (c): Data minimisation | ICO
[8] Principle (d): Accuracy | ICO
[9] The right to rectification | ICO (UK GDPR Guidance); The right to rectification | ICO (Law Enforcement Processing Guidance)
[10] Principle (e): Storage limitation | ICO

original purpose of the processing. As with the 'accuracy' principle above, this will be an important consideration when determining the underlying technology of a CBDC core ledger and the personal data processing involved. For example, the storage limitation principle could be difficult to reconcile with indefinite data retention that can occur on a blockchain. Questions around how long personal data will be stored, and the circumstances in which it is deleted in line with 'right to erasure' requirements, will need to be considered during the design process.[11]

- **Integrity and Confidentiality (Security)[12]:** This principle requires that data is kept safe and secure – with appropriate processes and protection in place against unauthorised and unlawful processing, and accidental breaches. There have been several well publicised breaches, exploits, hacks and compromises of ledger technologies.[13] The confidentiality, integrity and availability of systems and services therefore needs to be a priority. As the consultation notes, a highly secure, protected and resilient core ledger is crucial to a CBDC, not least for ensuring public trust and confidence.

- **Accountability[14]:** this principle places a clear onus on data controllers to be responsible for – and be able to demonstrate – compliance with the wider data protection principles. When further developing policy positions and designing a CBDC it will be important to map out the relationships between the participants in the ecosystem and their respective data protection obligations and responsibilities. This will provide clarity around which entities will be data controllers or joint controllers, and who will be data processors[15], and will help ensure that the division of accountability for data protection compliance is clear in the CBDC ecosystem.

9. In addition to the UK GDPR principles above, HMT and the Bank will need to consider how other specific elements of data protection law apply to CBDC design and deployment. For example, an important consideration during the design phase would be a focus on the access that law enforcement agencies will have to CBDC data. To help build and maintain public trust, the following should be taken into account:

[11] Right to erasure | ICO (UK GDPR Guidance); The right to erasure and the right to restriction | ICO (Law Enforcement Processing Guidance)
[12] Principle (f): Integrity and confidentiality (security) | ICO
[13] ICO Tech Horizons Report December 2022, p. 54.
[14] Accountability principle | ICO
[15] The ICO has guidance available on data controllers and data processors. See: Controllers and processors | ICO

- How the **six law enforcement data protection principles** under Part 3, Chapter 2, of the *Data Protection Act 2018*[16]*,* which set out the main responsibilities for competent authorities[17] to follow for law enforcement personal data processing, might apply to a CBDC.

- How organisations engaging with the CBDC core ledger, such as PIPs and those responsible for operating the ledger, will undertake **sharing of personal data for law enforcement purposes** with a competent authority in compliance with data protection law.[18]

- How any future **UK data protection and digital identity legislative reforms** – namely the *Data Protection and Digital Information (No. 2) Bill* – relate to the processing of personal data that could be undertaken within a CBDC ecosystem.

- How any **data protection requirements for international transfers** could apply to cross-border payment transactions that could arise within a CBDC ecosystem.[19]

10. The ICO also notes that there will be cyber security considerations – that are broader than impacts on personal data – which are relevant to a CBDC. Consideration of the security of the infrastructure and network relied upon to deliver any proposal will be important. These considerations should include the robustness of third parties in any supply chain supporting CBDC. The ICO presently oversees 'relevant digital service providers', including cloud computing services under Network and Information Systems Regulations 2018 (NIS) and the type of security requirements provided for in NIS are an important consideration when designing any future CBDC.

---

[16] These principles are broadly the same as those in the UK GDPR, and are compatible so data controllers can manage processing across the two regimes. The principles require that any processing of personal data for law enforcement purposes must be:
- **lawful and fair**;
- for a **specified, explicit and legitimate** law enforcement purpose;
- **adequate, relevant and not excessive** in relation to the purpose;
- must be **accurate** and where necessary, **kept up to date**; and
- **kept for no longer than is necessary** for the purpose for which it is processed;
- processed in a manner that ensures **appropriate security** of personal data.

See: Principles | ICO

[17] A "competent authority" is either a body listed under Schedule 7 of the DPA 2018 (the list includes policing bodies, bodies with investigatory functions, bodies with functions relating to offender management, government departments and other bodies) or a body which has a "statutory function" for one of the law enforcement purposes.

[18] For more information on the data protection legal frameworks that apply to data sharing for law enforcement purposes see: data-sharing-a-code-of-practice-1-0.pdf (ico.org.uk); Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the GDPR and Part 2 DPA 2018 | ICO

[19] See: A guide to international transfers | ICO

ICO response to consultation questions

Question 3: Do you agree that the Bank should not have access to users' personal data, but instead see anonymised transaction data and aggregated system-wide data for the running of the core ledger? What views do you have on a privacy -enhancing digital pound?

11. The consultation paper[20] sets out a number of positions regarding personal data processing that would shape the design of CBDC, including:

    - that neither the Government nor the Bank would have access to digital pound users' personal data.

    - that law enforcement agencies would have access to personal data under limited circumstances, prescribed in law, and on the same basis as currently with other digital payments (meaning a CBDC would not be anonymous, like cash).

    - CBDC users would – outside of these limited circumstances – only be known to and interact with their PIPs, who would be responsible for identifying and verifying users, and anonymising their personal data before sharing with the Bank's core ledger[21].

    - the Bank would have access to anonymised transaction data, and aggregated system wide data, which provides an overview of the total transactions (eg volume and value) taking place over a given period.

12. The consultation also emphasises that it is crucial, from the Bank's perspective, that information shared by PIPs with the Bank is anonymised and not personal data as defined under data protection law.[22] If the Bank does not need to use personal data to achieve its objectives – such as supporting innovation and improving the provision of services to PIPs and CBDC users –it should seek to use anonymous information instead, in accordance with the principle of

[20] See: The digital pound: a new form of money for households and businesses? Consultation Paper (bankofengland.co.uk), Section D.2.
[21] We note that no decisions on the underlying technology of a core ledger have been made, and that the core ledger operated by the Bank might run as a centralised traditional database, or might use distributed ledger technology like blockchain.
[22] Section 3(2) of the *Data Protection Act (DPA) 2018* states that **personal data** means: 'any information relating to an identified or identifiable living individual'. Section 3(3) defines an 'identifiable living individual' as: 'a living individual who can be identified, directly or indirectly, in particular by reference to (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.'

data minimisation (noting that, where information is not personal data, data protection law does not apply). The way in which PIPs convert personal data into anonymous information[23] – ensuring the risk of re-identification is sufficiently remote – so that it falls outside the scope of data protection law, will be a critical CBDC design consideration.

13. The data protection law definition of 'personal data', as well as ICO guidance concerning anonymisation, pseudonymisation and privacy enhancing technologies, will need to inform these design considerations.[24] A particularly important consideration will be whether data being processed by the Bank has undergone pseudonymisation[25], rather than anonymisation. Pseudonymised data is still personal data and data protection law applies.

14. Clarity and transparency about the personal data processing being carried out by different parties will be critical to building and maintaining public trust in any future CBDC ecosystem. When anonymisation of personal data is intended, the Bank will need to carefully consider how and whether the techniques that are applied are effective and reduce identifiability to a sufficiently remote level.[26]

Question 4. What are your views on the provision and utility of tiered access to the digital pound that is linked to user identity information?

15. The consultation proposes that CBDC users could choose from a range of wallet services with varying levels of identification requirements.[27] This tiered approach would allow for different levels of user access and functionality based on the amount of identification a user is willing or able to provide. The stronger the identification information a user provides, the greater the range and value of payments they would be able to make. It is also suggested that the private sector would provide basic access to a digital pound – with limited identification

[23] Data protection law does not explicitly define 'anonymous information'. However the ICO provides guidance that **anonymous information** must be ' …information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.' See: anonymisation-intro-and-first-chapter.pdf (ico.org.uk)
[24] ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance | ICO
[25] **Pseudonymisation** means that individuals are not identifiable from the dataset itself, but can be identified by referring to other information held separately. See: anonymisation-intro-and-first-chapter.pdf (ico.org.uk), pp. 15 - 16
[26] For more information on ensuring effective anonymisation see: Chapter 2: How do we ensure anonymisation is effective? (ico.org.uk)
[27] The ICO notes the importance of digital ID regulatory frameworks to financial services. We are working closely with the Government to further their commitment to using secure and trusted digital ID products in the UK. This includes helping the Government take a data protection by design and default approach to its trusted digital ID system.

verification, consistent with existing identification legal requirements for cashless payments – for users that do not wish, or are unable, to provide additional identity information.

16. ICO research shows that 59% of the public say that they are not fully aware of their choices around data sharing online and 81% feeling that it is important that they are given options to opt in and opt out of providing access to their data.[28] People need to be able to understand their information rights so they can decide how best to use and trust any new CBDC products and services. If designed well, tiered access wallets could increase user awareness and control over how and why personal data is processed in a CBDC ecosystem. Achieving this will hinge on people genuinely engaging with wallet choices, and understanding the privacy and payment benefits different tiers of access provide. Further research into consumer attitudes and demand concerning tiered access wallets should be carried out to inform CBDC design, with a view to ensuring people – including more vulnerable members of society – are able to choose and use wallets while remaining confident their information rights will be respected.

17. Data protection considerations will also need to inform the design and deployment of tiered access to wallets. Article 25 of the UK GDPR outlines obligations concerning 'data protection by design and by default'. This requires putting in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.[29] For example, the UK GDPR principles of 'Lawfulness, Fairness, Transparency', and 'Purpose Limitation' will be key to ensuring users can understand how and why identity information is used, and are protected from inappropriate re-use or repurposing.

Question 5. What views do you have on the embedding of privacy-enhancing techniques (PETs) to give users more control of the level of privacy that they can ascribe to their personal transactions data?

18. The ICO supports the use of PETs to give users more control over the level of privacy that they can ascribe to their personal transaction data. PETs can also help protect user privacy and support fulfilment of data protection obligations more broadly. We note that the Bank is still

[28] 20220124 Accent PPT summary of wave 2 quantitative and qualitative research (ico.org.uk), pp. 8-9
[29] Data processing by design and default | ICO

in the process of exploring potential PETs which could be used in a CBDC ecosystem and look forward to engaging further on this topic.[30].

19. The ICO has released guidance specifically focused on PETs.[31] Their use can help uphold 'data protection by design and by default' obligations set out in data protection law and we welcome the references to these requirements in the consultation and working paper. More specifically, the use of PETs could enable further analysis of personal data within a CBDC ecosystem while reducing data protection risks. There are, however, risks to consider when using PETs, including:

    - The potential lack of maturity of technologies in terms of scalability, availability of standards, and robustness to attacks.

    - A lack of expertise when not using an 'off the shelf' product (PETs can require significant expertise to set up and use appropriately).

    - Mistakes in implementation of a PET that can lead to risks to individuals' rights and freedoms.

20. While PETs can help provide an appropriate level of security and confidentiality for processing, they should not be regarded as a 'silver bullet' for data protection compliance. Our guidance makes clear that personal data processing must still be lawful, fair and transparent, and in alignment with the broader data protection principles.

21. Data protection impact assessments (DPIA) will be useful for guiding considerations about anonymisation techniques and the use of PETs within a CBDC ecosystem, as well as addressing data protection risks and ensuring compliance more broadly. While data controllers must carry out DPIAs for processing that is likely to result in a high risk to individuals, it is also good practice to complete an assessment of any major project that requires the processing of personal data.[32]

Conclusion

22. High standards of data protection for any future CBDC infrastructure – and the organisations operating within the CBDC ecosystem – will be critical to building (and maintaining) public trust and engagement with new products and services. If the public loses confidence in PIPs, or

[30] The digital pound: Technology Working Paper (bankofengland.co.uk) p. 24.
[31] Privacy-enhancing technologies (PETs) | ICO
[32] Data protection impact assessments | ICO

the security and confidentiality of their personal data in the CBDC ecosystem as a whole, this trust will be significantly undermined.

23. The ICO welcomes the emphasis the consultation places on data protection, and its recognition of the opportunities for CBDC design to ensure enhanced privacy functionality and support user control of personal data when using digital money. We look forward to further engagement with the Bank and HMT as they develop their CBDC policy positions.