The Information Commissioner's Response to the Financial Conduct Authority's call for input on the 'Potential competition impacts from data asymmetry between Big Tech firms and firms in financial services'

About the Information Commissioner

1. The Information Commissioner 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 Information Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and takes appropriate action where the law is broken.

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 Financial Conduct Authority's (FCA) Call for Input (CFI) focuses on the risks of financial services markets developing in a way that means there is data asymmetry between big tech[2] firms and other firms in financial services, leading to adverse effects on competition.

[1] ico25-strategic-plan-0-0.pdf,
[2] The FCA define 'Big Tech' firms as 'large technology companies with established platforms and extensive customer networks' in their October 2022 discussion paper: FS23/4: Potential competition impacts of Big Tech entry and expansion in retail financial services | FCA. We use the term 'Big Tech' in this broad sense throughout our response.

5. This focus is of strategic importance to the ICO. Our ICO25 plan sets out how the regulations we oversee support consumers to trust and confidently participate in the digital economy, including data-driven financial services markets. As we noted in our response to the FCA's 2023 Discussion Paper[3], the prominent role 'Big Tech' plays in the digital economy – and the scale and scope of personal data these firms collect and use – means that their processing activities can have significant impact on the public, from both an information rights and competition perspective.

6. We welcome the opportunity to further engage with the FCA on the potential impacts of big tech firm participation in financial services markets. This response provides the ICO's view on how certain elements of data protection regulations not only protect people's fundamental information rights, but also work in synergy with competition objectives to help mitigate potential data asymmetries between big tech firms and other firms in financial services.[4]

Re-use and re-purposing of personal data

7. Data protection law requires organisations that process personal data to adopt a 'data protection by design and by default' approach to the development of products and services that rely on personal data processing.[5] As part of applying this approach, a key consideration for organisations, including big tech firms and other firms in financial services, is the fundamental data protection principle of Purpose Limitation set out in Article 5(1)(b) of the UKGDPR.[6]

8. As the FCA's CFI highlights, this principle sets requirements regarding the re-use or repurposing of personal data collected and processed for one purpose (such as the provision of the core elements of big tech firms' digital services) and subsequently used for another (such as the provision of a financial product). It requires that organisations:

    - must be clear about what their purposes for processing are from the start,

[3] See: ico-response-to-fca-discussion-paper.pdf
[4] **This addresses question 3 in the FCA's CFI:** Are there regulatory (or other) constraints that mitigate or prevent: a: the asymmetry of data between Big Tech firms and other firms in financial services, or b: the adverse impact of this data asymmetry on competition? See: Call for Input: Potential competition impacts from the data asymmetry between Big Tech firms and firms in financial services (fca.org.uk), p. 11.
[5] See: Data protection by design and default | ICO
[6] See: Principle (b): Purpose limitation | ICO

- need to record their purposes[7] and specify them in privacy information for individuals, and
- can only use personal data for a new purpose if either this is compatible with an original purpose, consent is obtained from the individual, or there is a clear obligation or function set out in law for this processing.

9. Where an organisation wants to repurpose data, and a new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely to be incompatible with the original purpose. When in this situation, organisations are, in practice, likely to need to ask for specific user consent to use or disclose data for the new purpose.

10. The purpose limitation principle is an important protection, ensuring that organisations' reasons for obtaining personal data are open and clear and that what is done with the data is in line with peoples' reasonable expectations. This gives people agency about how their personal information is used, empowering them to exercise their information rights.

11. There could be circumstances where people do not want personal data held by big tech firms (such as their social media, shopping or search history) to be reused or repurposed in relation to a financial product or service. This personal data processing could be a source of competitive advantage for big tech firms, for instance, if the data collected from their large user base helps them develop advanced analytics and AI technologies, as well as allowing them to better tailor products and services based on insights about the needs and preferences of platform users. Purpose limitation requirements to seek specific consent for this data repurposing therefore places a constraint on the ways in which personal data access advantages contribute to asymmetries between big tech firms and competitors.

12. Purpose limitation requirements to seek specific user consent work in unison with other fundamental data protection principles to ensure users have clear information about what personal data is collected and how it is used. This includes the Lawfulness, Fairness and Transparency principle, and requirements under UK GDPR where consent is the lawful basis for processing.[8] Together, these requirements on organisations support people to engage with and

[7] Data controllers need to specify the purpose or purposes for processing personal data within the documentation they are required to keep as part of their records of processing obligations under Article 30.
[8] See ICO guidance: Lawfulness, fairness and transparency | ICO; What is valid consent? | ICO. .

make an informed decision over whether to accept the terms offered by firms for the use or reuse of their personal data. This helps foster healthy competition that benefits users, since it can help reset the balance between digital businesses and users, putting the onus on the business to do more to engage users and give them greater benefit from personal data processing.[9] This helps ensure that users have greater insight and control over how their personal data is processed, and are empowered to exercise their information rights.

Personal data access and sharing

13. The CFI notes that if competitor firms can access the data provided by big tech firms, or sufficiently gain similar insights based on other available datasets, the competitive disadvantage created via data asymmetry may not exist as strongly. Therefore, regulatory interventions that enable the secure sharing of data with authorised third parties at a customer's request – such as future open finance or Smart Data schemes – have the potential to mitigate adverse effects on competition.

14. Data protection legislation enables the responsible and lawful use and sharing of personal data, which can drive innovation, competition and economic growth. Accordingly, the ICO engages extensively with industry, other regulators and Government on potential data sharing scheme proposals.[10] Key legal requirements such as the data protection principles,[11] obligations relating to a 'data protection by design and by default' approach,[12] and the importance of assessing and minimising risks (including through Data Protection Impact Assessments[13]) should shape the design of such schemes in ways that promotes trust and transparency.

15. Also relevant to data sharing schemes is the Right to Data Portability, set out in Article 20 of the UK GDPR. This provision gives individuals the right to obtain the personal data they have previously provided to an organisation, and reuse it for their own purposes across different services.[14] It gives people the right to receive this personal data in a

---

[10] The ICO's response to government's consultation on a potential 'Open Communications' scheme outlines our previous engagement. See: response-to-dsit-open-communications-consultation.pdf (ico.org.uk), p. 7.
[11] See: A guide to the data protection principles | ICO
[12] See: Data protection by design and default | ICO
[13] The ICO recommends that a Data Protection Impact Assessment is undertaken for any major project that requires the processing of personal data. See: Data Protection Impact Assessments (DPIAs) | ICO
[14] It is important to note that the Right to Data portability only applies when the lawful basis for processing information is consent or performance of a contract, and the processing is carried out by automated means (ie excluding paper files). See ICO guidance for further information: Right to data portability | ICO

structured, commonly used and machine readable format. It also gives people the right to request that an organisation transmits this data directly to another organisation.

16. Any future open finance or Smart Data schemes could provide enhanced data portability opportunities that go beyond Article 20, such as by guaranteeing the transfer of customer data in real time, or in specific useful formats. This would complement Right to Data Portability requirements if implemented in line with data protection law. Data sharing, when undertaken within the guardrails of UK data protection law, can enable better consumer choice and control and has the potential to mitigate power imbalances between firms holding large scale data sets and those seeking to use them.

Conclusion

17. Data protection and competition objectives share strong synergies. Regulatory efforts that seek to mitigate power asymmetries and promote user autonomy, choice and control in data-driven markets can support information rights and healthy competition. The ICO looks forward to continued cooperation with the FCA to promote these interests as it considers the issues raised through this CFI – both bilaterally and through the Digital Regulation Cooperation Forum (DRCF).[15]

[15] See: About the DRCF | DRCF