Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to the International Trade Committee Inquiry into Digital Trade and Data

1. The Information Commissioner's Office (ICO) has responsibility in the UK for promoting and enforcing the General Data Protection Regulation (UKGDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003, amongst others.

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 does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken. The ICO welcomes the opportunity to respond to the International Trade Committee's call for evidence on Digital Trade and Data.

Introduction

3. The use of personal data is central to digital services and to digital trade. In recent years we have seen transformational changes in how personal data is used in digital services and products. Moreover, the Covid-19 pandemic has driven an acceleration in the uptake of digital services that would otherwise have been expected to take years. The UK has a growing digital economy and this goes hand in hand with growth in data flows across borders and innovative uses of personal data.

4. Personal data is transferred and exchanged in many parts of the digital economy, including:

    - Use of apps and online services located in different parts of the globe.
    - Cloud storage services that support data analytics and Artificial Intelligence (AI).
    - Global financial services.
    - Employees' data in multinational companies.
    - Digital marketing services.

5. For the UK public these data flows sit seamlessly behind the services they use and it is difficult to understand where in the world their data is sent, processed and stored.

6. The full potential of the digital economy will be realised by fostering trust, which is underpinned by the application of high standards of data protection. The public can quickly disengage from digital services when they lose confidence in how their data will be protected. Trust therefore plays a vital role in allowing the flows of data between countries upon which international trade is based.

7. UK data protection law can support and enable digital trade agreements and should not be regarded as a barrier. The UKGDPR, derived from EU GDPR, seeks to enable data flows via measures to protect personal data when it is transferred to a third country.

8. There are a range of measures in the UKGDPR, from an assessment of the third country's data protection system (known as adequacy) to standard contracts and certification. Regulatory cooperation between data protection authorities around the globe can also support this system in practice. The ICO believes that UKGDPR can work effectively to protect data in a way that is compatible with trade agreements.

9. Outside of the trade context, the ICO also supports the adoption of international standards of data protection, based on recognised international standards such as the Privacy Guidelines of the Organisation for Economic Cooperation and Development (OECD) and Convention 108 of the Council of Europe. International high standards are essential to maintaining trust in digital trade and between different data protection jurisdictions.

10. Around the world, data protection standards are converging towards higher data protection standards and becoming more interoperable – as evidenced by a new law in Brazil, the new Data Protection Bill in India and reforms happening in New Zealand, Canada and Australia. A debate is also underway about Federal Privacy law in the US.

11. It is important to recognise that there are a number of ways countries around the world may seek to meet high data protection standards and there should be space for different cultural, legal and constitutional approaches, alongside a move towards common principles. What these

developments evidence when taken together however is a wider consensus on the desirability of high standards.

The role of the ICO in enabling data flows and protecting data across borders

12. The ICO recognises the importance of a thriving digital economy to the UK and the financial and societal benefits that this can provide. We can assist with this objective for growth by providing guidance to business to help them comply with their obligations, supporting innovation with initiatives such as our data protection sandbox, which provides a safe space for regulatory advice on building data protection into innovative digital projects and services. This approach seeks to support and enable compliance first. The ICO also has the capability to take enforcement to address systemic and non-compliance that create significant risks for the public.

13. This twin-track approach ensures there is a level playing field for businesses – helping organisations to understand and meet their data protection obligations while targeting poor behaviour with proportionate regulatory action.

14. We are also working to support businesses that depend on data flows with the EU. The ICO continues to provide expert, independent advice to Government in its work to obtain a positive data adequacy decision from the EU, which will secure an effective and straightforward system for the transfer of data to the UK. We are aware that for many organisations, particularly small and medium sized-enterprises (SMEs), adequacy provides the most advantageous option, both in terms of consistency and cost. Adequacy enables free flow of data with no further measures required of organisations.

15. This is complemented by the ICO's provision of advice and guidance to businesses on the use of other transfer mechanisms, such as standard contractual clauses and binding corporate rules. The ICO is also developing other mechanisms, such as industry codes and certification schemes, as ways of continuing to be able to transfer data across borders.

Committee questions

What are the main barriers faced by UK businesses engaging in digital trade?

16. Our experience in providing regulatory advice and guidance has taught us that businesses want clarity and consistency in the rules that they must follow, particularly when they are operating in multiple jurisdictions. Interoperability of the regulatory regimes in those jurisdictions is also of great importance, as it allows businesses to consolidate their approach and thereby reduce costs and risk whilst providing more effective protection for their customers.

17. Global digital trade is underpinned by cross-border data flows. The use of cloud services is now commonplace at all organisational levels, from small businesses looking to create a trading website to cutting-edge technology such as AI systems employed in both private and public sectors. Complex cross-border data flows are therefore a fact of daily life in the modern world.

18. Businesses also recognise the value that high data protection standards can have in creating trust and confidence in their services, both from consumers and other businesses they work with across borders.

What opportunities does digital trade present for UK businesses?

19. Effective protections for privacy and data protection are a cornerstone of a modern digital economy, essential to fostering the trust required for digital and non-digital services to thrive.

20. The UK therefore has a strong opportunity to build on the high standards of the UKGDPR and the regulatory innovation of the ICO to create trust globally in data flows and in and out of the UK. This in turn could make the UK ideally placed to lead in digital services and become a hub of digital trade.

How does the regulation of digital trade impact consumers?

21. It is important for regulators in different jurisdictions to co-operate with each other to create a framework in which consumers can be confident that their data will be safe and not used in ways which could cause them harm. For example, when an individual in London decides to download an app to help them find a good restaurant, they do not expect to have to check where in the world the app developer is based, and what privacy protections that country provides.

22. The public will expect the UK protections to follow the data, to an equivalent standard, when their data is transferred overseas. Trust in this process can also enable UK consumers to enjoy diversity and choice in digital services.

23. It is also increasingly clear that there is an intersection between data protection and other concerns and areas of regulation; for example, in the areas of online harms, use of algorithms and AI, consumer protection, competition and financial services regulation. There is therefore a need for collaboration, both between domestic regulators and, given the global nature of the digital economy and trade, across borders.

24. Regulatory cooperation enables data protection to work across borders, to protect citizens. For example, the ICO has recently opened an investigation into the ClearView facial recognition technology service with the Australian Information Commissioner.

25. Trade Agreements related to digital trade and data can build on the regulatory cooperation foundations that exist in other contexts. The ICO has, for instance, concluded a Memorandum of Understanding with the Singaporean Data Protection Authority, to share good practice in areas of regulatory innovation.

26. The ICO currently chairs the Global Privacy Assembly (GPA), the global forum for data protection and privacy authorities. The GPA seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of more than 130 data protection and privacy authorities from across the globe. As Chair of the GPA, the ICO is leading work on greater regulatory cooperation related to the digital economy, including on issues such as facial recognition technology and privacy implications of digital currencies.

27. The desirability of working across regulatory frameworks associated with risk and harm is already recognised domestically in the development of the UK Regulators Network (UKRN) and Digital Regulation Cooperation Forum (DRCF) – involving the ICO, Ofcom and the Competition and Markets Authority. The UK is leading the way in this form of cooperation and there is an opportunity to use digital trade to advance the benefits, for the public and business, of this approach to regulatory coherence.

What approaches should the UK take to negotiating digital and data provisions – including those concerning the free flow of data, protection for personal data, net neutrality, data localisation, and intellectual property– in its future trade agreements?

28. In terms of precedent, trade agreements do not directly regulate data protection and data flows; domestic data protection law does this. The ICO's role is to regulate data protection law and we recognise the specific roles played by Government and Parliament in relation to trade agreements. The ICO will provide independent regulatory advice on the intersection between the data protection and trade.

29. Trade agreements can be used to support high data protection standards and may play a role in setting the wider framework in which domestic laws evolve. Traditionally the EU has not sought to address data protection in trade agreements, though the recent EU-UK Trade and Cooperation Agreement does address it. Agreements in Asia-Pacific have covered data protection, reflecting the growing importance of digital trade and trust.

30. It is therefore important to properly consider and understand the implications of any provisions in trade deals that cover privacy and data protection. This would include assessing whether key elements of the UK's domestic data protection framework could be impacted via a challenge under trade dispute mechanisms.

31. The ICO supports an approach to trade agreements where the parties agree to maintain high data protection standards. If trade agreements contain provisions that allow the parties to challenge data protection laws on the basis that they may place unfair restrictions on the transfer of data, there should be recognition of the importance of maintaining data protection laws and international data transfer requirements as a legitimate policy measure.

What does the UK-Japan Agreement indicate about the UK's approach to digital trade and data provisions in future trade negotiations?

32. The UK-Japan Agreement (the Agreement) includes provisions relating to data protection and flows of data. In Article 8.80 of the Agreement it explicitly recognises the societal benefits of protecting personal data and the contribution it makes to enhancing consumer confidence in commerce. Further provisions commit each side to adopting or maintaining a

framework for the protection of personal data that takes into account the principles and guidelines of relevant international bodies. As mentioned, trade deals are part of the framework in which domestic laws evolve and it is therefore important for them to recognise and reinforce the value of data protection.

33. This is the first deal of its kind for the UK. Accordingly, how the Agreement will interact with domestic data protection law must be understood. This is particularly the case as the Agreement may set a precedent for future trade deals that the UK strikes. We do not, for example, know how the provisions in Article 8.84 of the Agreement, covering restrictions on data flows, could theoretically be triggered by Japan, as there is little international precedent.

34. Having said this, we do not see significant risks for UK data transferred to Japan. Under article 8.84 the UK would clearly have a strong case that UKGDPR would constitute a 'legitimate public policy objective' and the protection required for transfers could be a justified restriction.

35. We also highlight the positive approach that Japan has taken to data protection with its "free flow of data with trust" initiative in international forums such as the G20 and OECD. We also note the changes that Japan has made to its own domestic data protection regime as part of the EU's data adequacy decision, which the UK has 'rolled over' with Japan's agreement. This includes protections for onward transfers, meaning that UK data is receiving an equivalent level of protection if transferred to Japan.

What objectives should the UK have when negotiating digital and data provisions during its accession to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)?

36. We note that the CPTPP contains similar provisions to those in the UK-Japan Agreement, recognising the importance of data protection to electronic commerce and committing all parties to implementing a data protection framework that takes into consideration relevant international standards.

37. We therefore believe that the CPTPP can be compatible with the UK's domestic data protection regime. However, it is important to study other international precedents to fully understand and consider the implications

of the CPTPP on the UK's domestic data protection regime and we are providing advice to the Government in this regard.

What domestic and international law is relevant to the Government's approach to digital trade?

38. The UK's domestic data protection regime is the culmination of over 35 years of development, and today provides UK citizens with world-leading levels of data protection. This framework is vital to the development of the digital economy.

39. The ICO welcomes the Government's commitment in its National Data Strategy to work with the ICO to develop cooperation with other national data protection authorities, to maintaining high data protection standards and to the need for the standards to stay fit for purpose in a rapidly developing technological environment.

40. To this end, we see significant benefit in the timely ratification by the UK of the modernised version of Convention 108 of the Council of Europe, also known as Convention 108+ (C108+). As C108+ is the only global treaty for data protection, with a potential to become an important global standard of the future for data protection, ratification of C108+ would reaffirm the UK's commitment to common global data protection standards. This, in turn, would make global data flows easier and therefore encourage global digital trade.

41. Similarly, the ICO recommends continued adherence to the OECD's Privacy Guidelines, which lay out the principles on which most modern data protection laws are based. First published in 1980, the Privacy Guidelines were developed in close cooperation with the Council of Europe as it developed what would become the original C108 and were the first internationally agreed statement of the core information privacy principles that are recognised globally today. They remain an important point of reference in policy discussions and have had a substantial impact, including as the basis for many national laws.

42. Nearly every OECD country now has one or more laws protecting privacy, and even countries outside the OECD often look to these guidelines when developing their own national data protection laws. The Privacy Guidelines are currently being reviewed to ensure they remain relevant and fit for purpose in today's increasingly globalised and digital world.