Information Commissioner's Office – Written evidence (FDF0017)

About the ICO

1. The Information Commissioner has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR). He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

ICO response

2. The Information Commissioner's Office (ICO) is pleased to take this opportunity to respond to the call for evidence from the House of Lords Committee on the Fraud Act 2006 and Digital Fraud (the Committee).
3. The Committee has posed a number of questions. In this response the ICO focusses on two questions, 8 and 7, respectively because these are most relevant to our remit.

Data protection - the UK GDPR and data sharing

4. Committee question 8. "What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, does General Data Protection Regulation (GDPR) limit data sharing?"
5. The EU General Data Protection Regulation (EU GDPR) has now been written into UK law as the UK GDPR. The UK GDPR and the DPA (together referred to as the data protection legislation) provide a legal framework that organisations must follow when processing personal data; data sharing is a form of processing. The legislation enables data sharing to take place in a fair, safe and transparent way.
6. Data sharing that complies with the law has several benefits, including the following:
    - It is a driver of innovation and economic growth.
    - It improves insights, such as research and analysis to support better decision-making.
    - It engenders public trust, as the public can have confidence that organisations are using their data safely.

7. This response sets out how, rather than being an impediment to sharing data, the framework provided by the data protection legislation facilitates fair, transparent data sharing that engenders public trust in organisations.

8. The ICO acknowledges that challenges exist outside the requirements of the legislation itself, and that some barriers remain to data sharing. The former Information Commissioner, Elizabeth Denham, highlighted this in her foreword to the data sharing code:

9. "This code demonstrates that the legal framework is an enabler to responsible data sharing and busts some of the myths that currently exist. But we cannot pretend that a code of practice is a panacea to solve all the challenges for data sharing. Or that targeted ICO engagement and advice will solve everything. There are other barriers to data sharing, including cultural, technical and organisational factors. Overcoming these will require more than just the ICO; it will require a collective effort from practitioners, government and the regulator."

10. The ICO emphasises that it continues to be keen to work with the committee, and with the government and others, to resolve these issues.

Practical guidance in the data sharing code

11. The ICO has produced a wealth of guidance[1] that helps organisations to understand and comply with data protection law. It has also produced the Data sharing code of practice[2] (the data sharing code): a statutory code made under section 121 of the DPA, providing practical guidance for organisations about how to share personal data in accordance with the law. The data sharing code underlines how data protection legislation enables responsible data sharing, and it aims to give confidence to organisations to share data by means of clear, practical guidance, links to further information, and real-life examples and case studies. The code is complemented by resources in a data sharing information hub[3].

12. The code contains examples and case studies relevant to a range of scenarios across the public and private sectors. Below is an example relating to fraud.

Data sharing required by law

A local authority was required by law to participate in a nationwide anti-fraud exercise that involved disclosing personal data about its employees to an anti–fraud body. The exercise was intended to detect local authority employees who were illegally claiming benefits that they were not entitled to.

Even though the sharing was required by law, the local authority still had to inform any employees affected that data about them was going to be shared and still had to explain why this was taking place, unless this would have prejudiced proceedings.

[1] Guide to Data Protection | ICO
[2] Data sharing: a code of practice | ICO
[3] Data sharing information hub | ICO

The local authority had to say what data items were going to be shared – names, addresses and National Insurance numbers - and to provide the identity of the organisation they would be shared with.

There was no need for the local authority to seek employees' consent for the sharing because the law says the sharing could take place without consent. The local authority also had to be clear with its employees that even if they objected to the sharing, it would still take place.

The local authority had to be prepared to investigate complaints from any employees who believed they had been treated unfairly because, for example, their records had been mixed up with those of an employee with the same name.

13. The data sharing code takes organisations through the practical considerations when contemplating sharing data, explaining the benefits of these steps and featuring links to further guidance and other resources. A checklist[4] in the code is a helpful tool that sets out the main factors to consider. These factors are designed to help organisations and should not be seen as an impediment.

14. Data sharing to assess fraud risk is likely to involve law enforcement processing. The data sharing code explains data sharing for law enforcement purposes (under Parts 2 and 3 of the DPA) between competent authorities and other types of organisation in a dedicated section.[5] The data sharing information hub features a toolkit to help smaller organisations to share data with competent authorities.[6]

Cyber incidents and data subject notification

15. The Committee has also posed the following question:

    Question 7. "What are the responsibilities of the private sector in protecting the public against digital fraud? How can a balance be achieved between the need to tackle digital fraud whilst supporting the growth of these sectors? To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices?"

16. The ICO is conscious of the impact of digital fraud and has been working with other organisations to address it. The UK GDPR has a role here.

17. The ICO has seen a 19 per cent rise in reports of cyber security incidents involving people's personal data over the past two years[7]. A growing number of these cyber attacks come from phishing, with emails looking to trick or persuade people to share usernames and passwords. Such methods are commonly linked with fraud and may use information which has been gathered from other scams or data breaches.[8] The ICO actively engages with the the Home Office Cyber PROTECT working group. This group aims to oversee and provide strategic direction to Home Office work

[4] Annex A: data sharing checklist | ICO

[5] Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the GDPR and Part 2 DPA 2018 | ICO

[6] Can I share personal data with a law enforcement authority, such as the police? | ICO

[7] John Edwards, Letter to the Editor, Financial Times – 11 March 2022

[8] Fraud The Facts 2021- FINAL.pdf (ukfinance.org.uk)

on cyber PROTECT and associated work, contributing to the creation of a more joined-up response.

18. While individuals may be able to take some preventative action to protect themselves, they need to have trust and confidence that organisations hold their personal data securely. The UK GDPR requires organisations to process personal data securely by means of appropriate technical and organisational measures. This means implementing strong access controls, and for internet-facing services, using multi-factor authentication or similar strong access controls. Organisations also need to provide up-to-date training so that their staff can spot and report phishing attempts.

19. In addition, Article 34 UK GDPR requires controllers to notify individuals if their data has been compromised, where this is likely to result in a high risk to their rights and freedoms. One of the main reasons for telling individuals is to help them to take steps to protect themselves from the effect of a breach. Some organisations who report breach incidents to the ICO assess the likely risk as low, and therefore they do not inform the individuals concerned about what has happened to their personal data. In cases where the ICO considers that they have not properly assessed this risk, it explains to them why they should tell the individual about the incident and highlights ICO powers under article 34(4) UK GDPR to require them to do so.

Conclusion

20. The ICO trusts this evidence will assist the Committee, but is willing to contribute further on any specific points. As stated earlier, the ICO is happy to work with the committee, the government and others to overcome factors - such as organisational, technical and cultural - that may act as an impediment to data sharing.

21 April 2022