The ICO exists to empower you through information.

10th Floor, Causeway Tower, 9 James St South, Belfast, BT2 8DN
T. 0303 123 1114 E. ni@ico.org.uk
ico.org.uk

The Information Commissioner's response to the Department for Communities Revised Code of Practice on Obtaining Information.

Introduction

1. The Information Commissioner's Office (ICO) welcomes the opportunity to respond to the above consultation. This Office has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and additional information rights legislation.

2. This consultation relates to the Social Security Fraud Act (Northern Ireland) 2001 Code of Practice and is seeking views on proposed revisions to the code, which is set to replace the previous version, (issued in 2002).

3. It is our understanding that the code sets out proposals relating to the Department for Communities (DfC) powers to obtain information from certain organisations about their customers, to help deal with fraud against the benefit system.

4. It has been revised to take account of operational changes brought about by creation of the DfC's Benefit Security Division. Furthermore, we note that the revised code includes updates from recent legislation, clearer guidelines on information requests and disclosures, and enhanced safeguards for data security and retention.

5. We have detailed our feedback under the headings below.

Data Protection Act 2018 Principles

6. As stated, the draft Code of Practice outlines proposals that give DfC Authorised Officers the authority to obtain information from certain organisations about their customers to help deal with fraud against the benefits system. It is therefore likely that such processing will fall under Part 3 of the Data Protection Act (DPA) 2018.

Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510

10th Floor, Causeway Tower, 9 James St South, Belfast, BT2 8DN
T. 0303 123 1114 E. ni@ico.org.uk
ico.org.uk

7. Chapter 5 of this code sets out the safeguards that are in place to ensure that Authorised Officers do not misuse their powers. This chapter references the following key principles for law enforcement processing[1]: Lawfulness and fairness, integrity and confidentiality, and storage limitation.

8. It is important to note that the processing arrangements covered by this code will need to comply with ***all*** the key principles detailed in this section of the DPA 2018. This includes:

   - **Clear and legitimate purpose:** the data collected must have a clear and legitimate purpose, and it must not be used in ways that are incompatible with that original purpose.
   - **Adequate, relevant and not excessive:** the data must be limited to what is necessary for the purpose for which it is being processed.
   - **Accurate:** the data must be accurate and, where necessary, kept up to date.

9. This section of the code may benefit from being more explicit about the key principles that Authorised Officers need to take account of. For more information, please refer to this section of our website.

Sensitive Processing

10. We note that, when implementing the code, Authorised Officers may ask for information about people within a family in cases where their circumstances are relevant to the benefit claim being investigated.

11. As the code has been updated to reflect changes introduced by the Civil Partnership Act 2004, this will mean that Authorised Officers will be processing sensitive information (i.e. information pertaining to an individual's sexual orientation) for certain cases.

12. Due to this, clarity must be provided to Authorised Officers on their additional responsibilities and obligations regarding sensitive processing under Part 3 of the DPA. This includes the need to

[1] Outlined in Part 3, Chapter 2 of the DPA 2018.

Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510

meet at least one of the conditions set out in Schedule 8 of the DPA 2018 and to have an appropriate policy document in place.

Automated Processing

13. We note that the code has also been updated to reflect changes introduced by the Investigatory Powers Act (IPA) 2016. The IPA 2016 allows public authorities, law enforcement, and intelligence and security agencies to use automated systems and machine learning techniques to support their investigatory powers[2].

14. It is unclear whether the revised Code of Practice includes provisions for profiling or automated decision making. However, if the code does cover such processing, it is crucial to ensure that appropriate safeguards are in place. These safeguards should protect individuals' rights, particularly their right not to be subject to automated decisions that result in adverse legal effects or other significant impacts.

15. Clarity must therefore be provided to Authorised Officers regarding their responsibilities under Part 3 of the DPA when using automated systems for processing personal data. This includes ensuring that individuals under investigation have the right to obtain human intervention, express their point of view, and obtain an explanation of (and challenge) those decisions.

16. For more information, please refer to this section of our website.

Data Protection Impact Assessment

17. DfC should consider whether they need to carry out a Data Protection Impact Assessment (DPIA) to mitigate the processing risks linked to the draft Code of Practice.

18. DPIAs are a tool that can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows organisations to identify and fix problems at an early stage,

[2] This could include using algorithms to detect anomalies in large datasets that may indicate fraudulent activities.

Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510

10th Floor, Causeway Tower, 9 James St South, Belfast, BT2 8DN
T. 0303 123 1114 E. ni@ico.org.uk
ico.org.uk

reducing the associated costs and reputational damage which might otherwise occur.

19. They are not a mandatory requirement. However, a DPIA must be carried out before processing personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals. Processing that is likely to result in a high risk includes (but is not limited to):
    - systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals;
    - large scale processing of special categories of data or personal data relation to criminal convictions or offences;
    - using new technologies (for example surveillance systems).

20. DfC must consider the nature, scope, context and purposes of the processing when deciding whether it is likely to result in a high risk to individuals' rights and freedoms.

Authorised Officers

21. We note in Appendix 2 that the code contains examples of the types of information which can be requested by an Authorised Officer. However, it is unclear from the draft if all Authorised Officers will have the same level of information accessibility

22. DfC should consider whether they could improve the code's clarity by either confirming if this is the case, or if there is a difference to explain what these are, and how information providers can verify the level of authorisation an Authorised Officer has.

Third-Party Information

23. The revised code states that, "*The Authorised Officer must minimise any risk of obtaining information about innocent third parties."* Whilst the code goes on to state that the provider is not required to provide information in such circumstances, it does not advise Authorised Officers what to do in cases where they do obtain such information.

Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510

10th Floor, Causeway Tower, 9 James St South, Belfast, BT2 8DN
T. 0303 123 1114 E. ni@ico.org.uk
ico.org.uk

24. Authorised Officers should be advised (either through the code or through training) on what to do instances where they have been inadvertently sent such information.

Training

25. We appreciate the consultation's emphasis on the importance of staff training and that only staff who have undertaken the approved training will be allowed to make requests for information.

26. This is a key requirement under DfC's accountability obligations. Additionally, it is also essential that staff members receive practical data protection training tailored to their specific roles, with regular refreshers to ensure ongoing compliance.

Involvement of Data Protection Officer (DPO)

27. It is advised that DfC seeks expert advice from their DPO, (where relevant), during the drafting of this Code. Part of the DPO's role under the UK GDPR is to advise and inform their organisation of their obligations under data protection law.

Conclusion

28. We hope that the above comments are helpful. If there are any queries regarding our response or any points that require clarification, please do not hesitate to contact our office.

29. In addition, we are also happy to provide data protection advice and support to DfC when it comes to implementing the Code where it would be welcomed.

Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510