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 Cabinet Office's consultation on the expansion of the National Fraud Initiative Data Matching Purposes 2021

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). She 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 she can, and taking appropriate action where the law is broken.

Introduction

2. The Information Commissioner's Office (ICO) welcomes the opportunity to respond to this Cabinet Office (CO) consultation on the expansion of the National Fraud Initiative (NFI) data matching purposes, including its proposed amendments to the Data Matching Code (the draft Data Matching Code).

General comments

3. The UK GDPR and DPA enable processing that is fair and proportionate and the ICO recognises that there are important societal benefits that can arise from the use of personal data. Using data responsibly is vital to prevent harm and secure and retain the public's trust and confidence.

4. The ICO acknowledges that the proposed additional powers could help investigating authorities trace people of interest, track assets in proceeds of crime investigations and could also support the investigation of complex, serious and organised crime. Powers in relation to debt and error could also assist organisations in improved debt management and could be used to benefit individuals, by ensuring they receive the financial support they need, for example by being signposted to benefits.

5. Data protection legislation is not a barrier for legitimate and responsible data sharing and data matching, but the tools that are used need to be fit for purpose and proportionate. They also need to respect individuals' rights.

Summary of recommendations

6. The ICO's comments are set out in full below, but the following are our principal recommendations:

    - The need for accountability and a data protection by design and default, requiring:

        - the preparation of a data protection impact assessment (DPIA);
        - a clear description of the different data protection regimes which will apply when exercising each of the NFI powers;
        - compliance with the data protection principles and the provision of safeguards to mitigate risk to individuals;
        - the establishment of the respective responsibilities of the CO and any third party controllers involved in the NFI data matching exercises; and
        - particular attention to special category or sensitive data, criminal offence data, and children's data, where this is held.

    - Updates to the draft Data Matching Code to:

        - incorporate more detail about the data protection regimes which apply and the safeguards in place;
        - ensure the draft Data Matching Code is consistent with the ICO's Data Sharing Code;
        - ensure that the draft Data Matching Code is kept under further regular review; and
        - provide clear, practical guidance about how compliance with data protection legislation will be achieved.

Accountability and data protection by design and default

7. Accountability is an important aspect in engendering public trust and confidence, and the ICO has published an accountability framework to help

organisations demonstrate their compliance. The ICO recommends that the draft Data Matching Code should clearly reference the importance of accountability and signpost this ICO guidance[1].

8. A key aspect of accountability is being able to demonstrate a data protection by design and default approach to ensure that any risks in the processing of personal data are appropriately mitigated against and appropriate safeguards are put in place. This means integrating data protection in a project from the design stage and throughout the processing lifecycle.

9. Producing a DPIA is a process that helps controllers identify and minimise the data protection risks of a project, and ensure that it is compliant with the data protection legislation. The ICO regards it as good practice to undertake a DPIA in any large project involving the processing of personal data. A DPIA must be carried out before processing that is "likely to result in a high risk" to individuals. A DPIA must also be carried out if the processing includes automated decision-making which creates a legal or similar significant effect on individuals. The ICO has produced guidance that outlines when DPIAs are legally required, and how such assessments should be undertaken.[2]

10. If the DPIA identifies a high risk, and it is not possible to reduce that risk, the CO must seek prior consultation with the ICO on the DPIA before undertaking the processing.[3]

11. We note that the Cabinet Office has not yet undertaken a DPIA, although it intends to do so when piloting any of the proposed new powers. The ICO strongly recommends that the CO should carry out a DPIA as soon as possible and before any processing takes place, to ensure that data protection is central to the development of these proposals. This will ensure that data protection issues, including those highlighted in this response, can be identified, assessed and appropriately addressed. The case for a DPIA is further underlined because the NFI's data matching purposes potentially engage different data protection regimes for the CO and participating controllers including under UK GDPR/Part 2 DPA and Part 3

[1] Accountability Framework | ICO
[2] Data protection impact assessments | ICO
[3] Do we need to consult the ICO? | ICO

DPA (referred to in more detail below) which need to be carefully and separately considered.

12. In all cases, it will be important to establish with precision the personal data that is to be shared as this has a bearing on the principles discussed below.

The data protection regimes which apply

13. Part 3 of the DPA is separate from the UK GDPR regime. It applies to competent authorities (or their processors) processing personal data for the **primary** purpose of criminal law enforcement purposes. Competent authorities include the police and any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

14. When sharing data for law enforcement purposes with competent authorities, organisations who are not competent authorities themselves can rely on Part 2 of the DPA. In practice this means referring to UK GDPR, but, for example, a condition for disclosing the data may be required under Schedule 1 of the DPA or an organisation might need to rely on exemptions contained in the DPA.

15. In some instances, for example in relation to the powers to identify error, there may be no law enforcement component, in which case, the processing will take place under UK GDPR.

<u>Law enforcement processing under Part 3 DPA</u>

16. The processing of personal data for any of the law enforcement purposes will be lawful only if it is based on law and either the data subject has consented or the processing is **necessary** for the performance of a task carried out for that purpose by a competent authority.

17. Under Part 3 DPA, the processing must be:

    a) lawful and fair;
    b) specified, explicit and legitimate, and not processed in a manner that is incompatible with the purpose for which it was originally collected; and

c) adequate, relevant and not excessive in relation to the purpose for which is it processed.

18. If the NFI purposes are expanded as proposed, any processing for law enforcement purposes would be based on law. However, the competent authorities involved (including the CO, if applicable) would still need to explain why the processing is necessary. This means that the approach must be a targeted and proportionate way of achieving the purpose (in this case, the prevention or detection of crime/apprehension and prosecution of offenders).

19. For example, the new powers might mean that police forces can search local records from multiple sources more effectively, negating the need to make written requests under the DPA to separate authorities. Police or other competent authorities might regard the benefit as 'significant'[4], but the lawful basis will not apply if the purpose can reasonably be achieved by some other less intrusive means. Law enforcement authorities will also need to meet the threshold of strict necessity for the processing of any sensitive personal data, if this applies (see below).

20. In a blog published on 16 November 2018[5], the ICO discussed its investigation of the Metropolitan Police's 'Gang Matrix' (a database that records intelligence related to gang members). We found that although there was a valid purpose for the database, there were serious breaches of data protection laws with the potential to cause damage and distress to those on the matrix. This enforcement action is a good example of the need to balance the processing of 'intelligence' clearly against data protection law.

21. In any event, it will be necessary to consider the impact of the requirement under Part 3 DPA that, where relevant, and as far as possible, steps should be taken to distinguish between different categories of individuals such as suspects, individuals who have been convicted, victims and witnesses or other persons with information about offences (only information that is relevant to the investigation needs to be categorised). The draft Data Matching Code should set out how these issues should be addressed.

[4] Appendix 3 Paragraph 1.3 of the consultation

[5] Blog: Information Commissioner's investigation into the Metropolitan Police Service's Gangs Matrix concludes with enforcement action | ICO

22. It will also be necessary to consider the implications arising from the inclusion of any datasets in addition to those already listed. Police authorities are stated to be mandatory participants in the NFI data matching, and currently provide payroll, pensions and trade creditor information. The draft Data Matching Code needs greater clarity to establish whether police or other competent authorities will be required to provide any further datasets under these proposals, whether on a mandatory or voluntary basis.

Processing under UK GDPR (including processing under UK GDPR/Part 2 DPA)

23. Under UK GDPR, personal data must be processed fairly, lawfully and transparently.

24. The CO states in its present privacy notice for its NFI data matching activities[6] (the NFI privacy notice) that it relies on public task as the lawful basis for the proposed processing. If this remains the case, individuals' rights to erasure and data portability do not apply and this should be explained in the draft Data Matching Code, and the consequent impact on individuals considered in a DPIA.

25. Relying on public task as the lawful basis for processing means that the processing must be **necessary.** The consultation is framed in terms of the overall desirability of the proposed powers, but does not discuss the question of whether the CO can reasonably perform its tasks or exercise its powers in a less intrusive way. Additionally, and in the absence of a DPIA, the consultation does not suggest how processing under the proposed new powers might affect individuals and that the CO can justify any adverse impact.

26. For example, data from a range of datasets, including those from credit reference agencies, are included in the NFI data matching exercises. As a result of the current pandemic, and its adverse financial impact on individuals as well as the wider economy, there may be many more people in debt than previously. However, the consultation document does not explain how the proposed data matching, which accesses large data sets to search for individuals, is necessary and justified. For example, there are no guidelines to indicate how the use of data for the debt powers would be

[6] National Fraud Initiative privacy notice - GOV.UK (www.gov.uk)

balanced against the level of intrusion involved. There is no detail on how the level of an individual's debt might affect the matches and how those matches will be capable of being used.

27. The NFI data matching exercises give participants access to matches made against a considerable number of datasets, which together already amount to a significant amount of personal data. Further datasets can be added in the future. As a result of the expansion of the current powers, these data sets could potentially be interrogated more extensively, which means that the risk of an adverse impact on individuals is likely to rise. The CO needs to be able to identify that risk and show how it will be mitigated. A DPIA will help the CO to do this.

The application of the data protection regimes to NFI data matching exercises

28. Making clear which data protection regime applies is important because there are key differences between the provisions of the UK GDPR/Part 2 DPA and Part 3 DPA. These differences affect matters such as individuals' rights, the lawful basis for processing, and governance. It is important to note that these distinctions will already apply to the current purpose of fraud, as well as the new law enforcement purposes proposed.

29. In the draft Data Matching Code, the CO acknowledges that it is a controller for personal data processed in the course of NFI data matching activities under its statutory data matching powers under the Local Audit and Accountability Act 2014 (the 2014 Act). As a government department, the CO itself is a competent authority when its primary purpose for processing is for law enforcement purposes.

30. In its privacy notice for the NFI (the NFI privacy notice), the CO relies on UK GDPR to authorise its processing. However, the consultation documentation does not explain whether CO will continue to process personal data under UK GDPR and Part 2 DPA (utilising exemptions for law enforcement under the DPA, if required)[7] or whether it will be acting as a competent authority under Part 3 DPA under the new powers. The CO needs to clarify the regime which will apply to its own processing under the new powers.

[7] Schedule 2, Paragraph 2(1) DPA

31. Even if the CO continues to rely on UK GDPR/Part 2 DPA, other controllers involved in the NFI data matching exercises and those who draw on matches made by those exercises may need to rely on Part 3 DPA to authorise their processing and this should be clearly referenced in the draft Data Matching Code.

Ensuring compliance with data protection principles

32. A DPIA will help CO to consider whether the proposed processing would be compliant with the data protection principles. In particular, the CO will need to demonstrate the existence of safeguards to ensure that the data matching is fair, lawful and transparent, limited to specific purposes and no more than is necessary to meet those purposes.

33. Processing personal data fairly means that it should not be used in ways that individuals would not reasonably expect, or which would cause them unwarranted harm. As an example, police and other competent authorities must show that their processing is proportionate and relevant to their particular investigations. The CO may therefore need to consider how it can structure or restrict data matching in ways that ensure that the NFI data matching exercises remain focused on the conventional understanding of data matching, aimed at finding 'anomalies'.[8] Alternatively, it needs to be clear about what its purposes are and how it intends to use its data matching powers in practice in line with the purpose limitation principle. It will also need to consider how it will mitigate risk to individuals. Otherwise, the NFI exercises, including for example AppCheck which provides results 'on demand', could potentially allow participants to conduct disproportionate searches for information about particular individuals across a wide range of sources without lawful cause under data protection legislation.

Establishing responsibilities

34. A DPIA and the draft Data Matching Code should set out the respective responsibilities of the CO and any third party controllers.

35. Paragraph 2.9.5 of the draft Data Matching Code refers to Part 3 processing and links to the ICO's guide to law enforcement processing[9], but it would be helpful to see the respective responsibilities of the CO and any third party controllers more comprehensively explained and clarified in the draft

[8] Paragraph 2.6 and Appendix 2 of the draft Data Matching Code
[9] Guide to Law Enforcement Processing | ICO

Data Matching Code, particularly in relation to the different aspects of UK GDPR and DPA processing that might apply. This would ensure that everyone participating in the NFI data matching exercises, including the CO, is aware of and can address any differing requirements.

36. Additionally, there are likely to be important differences in approach depending on whether a third party controller is a mandatory or voluntary participant in NFI data matching exercises. For example, although a mandatory participant is obliged to comply with data protection legislation[10], in practice they may have no choice but to provide datasets to CO under the 2014 Act. In this case, the CO should explain its own role in ensuring compliance. This will include an assessment of the implications of the processing on an individual's rights as well as consideration of a controller's lawful basis for processing. For example, if a mandatory participant were to rely on legal obligation for their lawful basis, individuals will have no rights to erasure, data portability or to object to the processing.

37. Although the draft Data Matching Code is principally concerned with the CO's own approach to NFI data matching, there are intertwined responsibilities between all controllers involved. It would therefore be helpful for all these issues to be clearly addressed in the draft Data Matching Code. Where appropriate, the draft Data Matching Code could usefully contain links to other publicly accessible guidance, including ICO guidance, which addresses these issues more fully.

Special category data (UK GDPR) and sensitive data (Part 3 processing)

38. All competent authorities processing under Part 3 DPA will need to establish whether any of the personal data processed as part of the NFI data matching exercises under existing or expanded purposes is sensitive data[11]. If this is the case, they will need to be able to demonstrate that the processing is **strictly necessary** and also be able to satisfy one of the conditions in Schedule 8 DPA, unless the processing is based on consent. Strictly necessary means that the processing has to relate to a pressing social need which cannot be reasonably achieved through less intrusive means. If sensitive processing is being carried out, there must be an appropriate policy document in place.

[10] Paragraph 2.6.4 draft Data Matching Code and the 2014 Act
[11] Section 35(8) DPA

39. The CO needs to clarify whether it is processing sensitive data under Part 3 DPA. The NFI privacy notice refers to the lawful basis for processing 'sensitive' personal data as: '*processing is necessary for reasons of substantial public interest for the exercise of a function of the Crown, a Minister of the Crown, or a government department*'. This however is a condition for processing **special category** data, as defined under UK GDPR, and not sensitive data, as defined in Part 3 DPA.

40. Reliance on this condition for special category data under UK GDPR means that the CO also needs to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 DPA and demonstrate that the specific processing is necessary for reasons of substantial public interest. Further information about this should be set out and explained in the NFI privacy notice.

41. It is not the CO's current intention to mandate the use of patient data in the NFI data matching exercises, but the draft Data Matching Code allows for its use if required from a mandatory participant[12]. If this is under consideration now or in the future, careful consideration will be needed to ensure that there are the required safeguards for sensitive/special category data, in addition to compliance with any other legal, regulatory or common law principles that might affect its use.

Criminal offence data

42. The NFI privacy notice currently states '*Should data matching through the NFI result in a prosecution, then this may also be recorded by participating organisations*'. It also states that CO's lawful basis for processing '*criminal convictions data*' is paragraphs 6 and 10 of schedule 1 of the DPA. It is not clear from this notice whether and how, in practice, criminal offence data is being processed by the CO in the NFI data matching exercises. The consultation also does not explain if criminal offence data would be included in the exercise of any new powers.

43. We recommend that CO explains the circumstances in which criminal offence data would be processed, for example, clarifying if it will be processed for the purposes of collecting debt or for the proposed new law enforcement powers. The CO will also need to set out the measures to be employed to safeguard its use in the NFI privacy notice and the draft Data Matching Code.

[12] Paragraph 2.8.3

Children

44. Children merit special protection under data protection legislation. The CO will need to ensure that there are safeguards in place to ensure compliance with all data protection principles, and, in particular, fairness, if children's personal data is included in the NFI data matching exercises.[13] The CO will also need to consider how it can ensure that participants do not submit personal data from children for data matching, if this is the intent. These matters need to be considered and assessed in the DPIA, and discussed in the draft Data Matching Code and any accompanying guidance for participants.

Updating the Data Matching Code

45. The ICO has made comments above about a number of matters regarding the different data protection regimes which might apply to the CO and other controllers and which should be included in the draft Data Matching Code. The following points are of more general application:

Review of the Data Matching Code

46. The 2014 Act[14] requires the CO to continuously review the code and consult stakeholders before it is altered. It would be helpful to consolidate the references to the need for a review which appear throughout the draft Data Matching Code. This could also address issues such as the frequency of any review, the triggers for a review (such as changes in circumstances, need or practice), and how engagement with relevant stakeholders, such as the ICO, will take place.

ICO's Data Sharing Code of Practice

47. The Information Commissioner's Data Sharing Code of Practice (the Data Sharing Code) has been published[15] and will become a statutory code when it has been laid before Parliament. All organisations involved in processing personal data in connection with NFI data matching exercises will need to take the Data Sharing Code into account when sharing personal data.

48. The Data Sharing Code will apply to the CO itself and all organisations that share data as part of the NFI data matching exercises, whether on a

[13] Children | ICO
[14] 2014 Act, Schedule 9, paragraph 7
[15] Data sharing: a code of practice | ICO

voluntary or mandatory basis. It will also affect those participants who receive the results of these data matching exercises. Adhering to the Data Sharing Code will help to ensure good practice around data sharing and help to manage risks associated with sharing information, including the parties' approach to matters such as cybersecurity and individuals' rights. Following the Data Sharing Code and adopting its practical recommendations will give organisations confidence to collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information is being shared.

49. The ICO welcomes the references to the Data Sharing Code in the draft Data Matching Code. We recommend that the draft Data Matching Code is reviewed so that the approach to NFI data sharing contained within it is fully consistent with the Data Sharing Code.

Individual rights and freedom of information

50. As mentioned earlier, the draft Data Matching Code needs to make it clear which rights apply to individuals in respect of their personal data[16], noting in particular that these rights are not limited to an individual's right to be informed.

51. However, when referring to the right to be informed, there are only a few circumstances where controllers do not need to provide privacy information, so to suggest that this requirement applies 'so far as is practicable' might be misleading. Additionally, the checklist for privacy notices would benefit from a comparison with the checklist included in the ICO's guidance[17] to ensure that it is complete.

52. It is important to make it clear in the draft Data Matching Code that an individual's rights in relation to their personal data are not the same as the rights that arise under the Freedom of Information Act 2002(FOIA) which do not apply to personal data. It would therefore be helpful if these issues were discussed separately. The ICO has produced guidance in relation to freedom of information which will be of assistance and could be usefully signposted in the draft Data Matching Code.[18]

[16] See paragraph 2.18
[17] The right to be informed | ICO
[18] Guide to freedom of information | ICO

Datasets

53. Paragraph 2.6 of the draft Data Matching Code explains how the CO will choose datasets for matching. While it is acknowledged that new powers will be tested in pilots before rolling them out nationally, a requirement for 'reasonable evidence' does not appear to address the question of whether the processing is necessary or proportionate.

54. The draft Data Matching Code also needs to explain in greater detail, in the context of all NFI powers – new and existing - how the term 'significant'[19] is to be interpreted when testing the effectiveness of any data sharing. In this respect, the likely impact on individuals needs to be considered. This is likely to require an assessment of factors including the seriousness of any offence under investigation or disclosed in the datasets and the inclusion of any criminal offence data (which is also discussed above). There appear to be no guidelines currently in place showing how such factors will be balanced against the risks of intrusion.

55. In the same way, the draft Data Matching Code needs to explain the process through which CO decides that it is 'appropriate' to use data that has been provided voluntarily, and the criteria that will be applied when making that decision.[20]

56. It would also be helpful if a number of other terms were defined including:
    a. 'validate' and 'new information' (paragraph 1.2.4)
    b. 'fuzzy data matches' (paragraph 2.14.2)

Fairness

57. It is important to ensure that the Fairness Principles for data sharing under the debt powers[21] are not confused with the data protection requirement for fairness in processing undertaken as part of NFI data sharing exercises (whether under UK GDPR or Part 3 DPA). The draft Data Matching Code should therefore explain how specific fairness policies in relation to debt interrelate with the need for fair processing.

Accuracy and rectification

58. Given the purposes of the processing, accuracy is a particularly important principle under both UK GDPR and Part 3 DPA when applied to the NFI data

[19] Paragraph 2.6.3
[20] Paragraph 2.4
[21] Paragraph 2.3

matching exercises. The CO data deletion schedule[22] currently suggests inaccurate data should be deleted within three months of the inaccuracy being confirmed, but the processes and timeframes set out in the data deletion schedule or the draft Data Matching Code make no reference to the need for erasure or rectification without delay, or any safeguards to ensure inaccurate data is not transmitted (or if it is transmitted unlawfully, to ensure that the recipient is notified without delay).

59. In this respect, additional clarity would be helpful in paragraph 2.16.3 of the draft Data Matching Code regarding the requirement to consider notification of an error to an individual. As drafted, this gives a misleading impression that there is a requirement to report errors to the ICO as is the case for personal data breaches.

60. The draft Data Matching Code requires NFI participants to ensure the data submitted is of an appropriate quality and the ICO welcomes the detailed specifications published in relation to individual data categories on the NFI webpage.[23] CO says that other guidance can be found within a secure NFI site, but it would be helpful if there was publicly accessible guidance for participants about the practical steps that they may need to take to ensure data quality.

61. The draft Data Matching Code refers to the right to rectification by correction of errors from previous data matching exercises, but it does not refer to how errors in exercises in progress will be addressed, which could usefully be included in the draft Data Matching Code.

Retention

62. The CO has a data deletion schedule for the NFI data matching exercises and the draft Data Matching Code suggests that CO may be in the process of updating it. Data must be kept no longer than necessary, whether for the purpose of law enforcement or under UK GDPR. Appropriate time limits must be established for the periodic review of the continued storage of personal data. The information contained in the CO's current data deletion schedule and the other periods of time referred to in the draft Data Matching Code require coordination, particularly to clarify how ongoing investigations by those investigating data matches are factored into the

[22] The-NFI-Data-Deletion-Schedule.pdf (publishing.service.gov.uk)
[23] National Fraud Initiative: public-sector data specifications - GOV.UK (www.gov.uk)

retention timeframes, and also to ensure that the data is not retained inappropriately for long periods.

Accountability and security

63. The ICO's accountability framework[24] aims to help organisations of any size minimise the risks of what they do with personal data by putting in place appropriate and effective policies, procedures and measures. In this respect, the CO acknowledges the importance of ensuring that contracts with processors include technical and organisational security standards. However, it will be helpful to review current security measures, including those set out in the draft Data Matching Code,[25] against the key controls set out in the ICO's accountability framework.

64. There are also requirements for 'logging' as set out in Part 3 DPA[26] which require competent authorities operating automated processing systems to monitor and audit internal processing. This is to ensure that they know who they have shared data with, as well as allowing for monitoring of inappropriate access or disclosure of data, to verify the lawfulness of any processing and to ensure the integrity and security of personal data. The draft Data Matching Code would benefit from provisions setting out how these requirements should be fulfilled.

Profiling and automated processing

65. The draft Data Matching Code[27] and the 2014 Act make it clear that data matching cannot be used to identify patterns and trends that suggest nothing more than the individual's potential to commit fraud. The CO needs to undertake careful consideration of the profiling and automated processing that takes place as part of all the data matching exercises, including under any new powers. The statutory requirements under the 2014 Act and those of article 22 GDPR, where relevant, will need to be addressed in a DPIA which should highlight the impact of the new powers on any existing assessment of risk. It would also be helpful to see these considerations clearly articulated in the draft Data Matching Code, which should also highlight the particular requirements for accountability in respect of automated decision-making and profiling.[28]

[24] Accountability Framework | ICO
[25] Paragraph 2.12 and following
[26] S62 DPA
[27] 2014 Act, Paragraph 2.2.1 and Schedule 9, paragraph 1(5)
[28] Automated decision-making and profiling | ICO

Breach reporting

66. It would be helpful if ICO guidance about personal data breaches could be signposted in the draft Data Matching Code[29].

Review by the ICO

67. The present Data Matching Code refers to the potential for the ICO to be invited to undertake a review of the CO's data matching processes from time to time. It also refers to the potential for the ICO to be invited to review participants' procedures. These provisions are repeated in the draft Data Matching Code. Neither the CO nor any participants have approached the ICO to undertake such a review to date, but the ICO remains open to considering any such requests in future.

General

68. The email address to be included in the draft Data Matching Code and to be used for complaints to the ICO is icocasework@ico.org.uk and the telephone number for the ICO's helpline is 0303 123 1113.

Conclusion

69. The ICO looks forward to receiving a formal request for consultation from the CO in relation to these proposals, as required under Article 36(4) UK GDPR[30]. The ICO also welcomes continued engagement with the CO on the expansion of the NFI data matching purposes and on amendments to the draft Data Matching Code. As the CO continues to develop its work on these proposals through the use of pilots, as envisaged by the draft Data Matching Code, this could include engagement about the ICO Sandbox. When the required criteria for entry are met, this mechanism draws on ICO expertise and provides support to organisations that are developing products and services using personal data in innovative and safe ways.

Information Commissioner's Office

March 2021

[29] Personal data breaches | ICO

[30] Guidance on the application of Article 36(4) of the General Data Protection Regulation (GDPR) - GOV.UK (www.gov.uk)