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 public consultation from His Majesty's Revenue and Customs (HMRC): *Improving the data HMRC collects from its customers*

About the ICO

1. The Information Commissioner's Office (ICO) 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), 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). 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 provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and it takes appropriate action when needed.

2. The ICO supports the responsible use and sharing of personal data, particularly where this drives innovation and economic growth. We also aim to influence high standards of data protection and good information practices in the public sector.

3. The ICO welcomes the opportunity to respond to the HMRC consultation *Improving the data HMRC collects from its customers* (the consultation).

Summary

4. We recognise the important role that HMRC has as a custodian for data, when carrying out its functions as a tax authority, and the importance of it streamlining and improving its data collection, to assist with its ambitions for an effective, modern tax system. We also recognise the vital role that data can play in informing government's policy decisions and interventions, including proposals that might stimulate economic growth and deliver better public services across the UK.

5. Public trust and confidence are important factors in successful public sector initiatives involving personal data. Integrating high standards for

privacy and a positive approach to data protection when handling personal data are more likely to secure and maintain that trust and confidence.

6. A data protection by design and default approach will support HMRC in achieving these aims. This approach should include:

    - establishing the personal data in scope
    - undertaking a mapping exercise of the data flows involved
    - establishing the necessity and proportionality of the processing of personal data, building on fundamental principles of data protection
    - ensuring a fair and transparent approach that upholds and maintains individuals' rights
    - ensuring that appropriate protections are in place for any international transfers of personal data.

Background

7. The consultation seeks views on six potential areas where HMRC thinks that collecting additional data could bring significant benefits to customers and taxpayers. These are the business sector of the self-employed; the occupations of employees and the self-employed; the location(s) of an employment or business; the hours employees work; dividends paid to shareholders in owner-managed businesses; and the start and end dates of self-employment.

8. The data within scope of the proposals discussed in the consultation may include some information that does not relate to individuals and is therefore not personal data. Our comments are limited to issues relating to personal data and not to issues outside our remit.

9. HMRC's final decisions on whether it collects any or all of the proposed categories of data and how it then uses it will affect the data protection issues that arise and the potential for risk. We have therefore confined most of our comments at this time to overarching principles.

10. In particular, HMRC will need to be satisfied that it is necessary and proportionate in each case to collect the individual categories of the personal data that it proposes in this consultation, and that it does not collect more data that it needs. We therefore welcome further

engagement with HMRC to discuss specific data protection issues arising from the consultation in more detail, once it has reached settled positions on its proposals.

Data protection by design and default

11. HMRC will need to adopt a data protection by design and default approach when considering whether to collect more data from its customers and what those categories of data should be. Data protection by design and default is an overarching requirement of data protection law[1] and is vital when planning and investing in the responsible use of information. Data protection by design means considering privacy and data protection requirements at the earliest design stage of any system or service that will process personal data. This is particularly important if there will be new data sharing initiatives, or where organisations, including wider government, might use personal data for new purposes.

12. Keeping a data protection by design approach in focus throughout as HMRC considers its options for the data it collects will ensure that HMRC makes choices and develops its policies in a privacy enhancing way. This will not only help ensure compliance with the fundamental principles and requirements of data protection legislation, but will also assist HMRC (and any other organisations with whom HMRC might share data) in demonstrating their accountability for their processing of personal data.

Personal data

13. HMRC will need to clarify the personal data in scope of these proposals as this will affect whether the data protection legislation applies to some or all of its activities. Therefore, as an essential preliminary step, HMRC will need to consider the extent to which, in the various options it sets out, some or all of the information it plans to collect could relate to individuals.

Data protection impact assessment

14. A data protection impact assessment (DPIA) is a useful tool to help organisations identify risk and assess potential mitigating steps. Undertaking a DPIA at an early stage will support a data protection by

[1] Article 25 UK GDPR

design approach to the collection of each and any category of additional data and will help identify areas of risk. It is also important to note that a DPIA is mandatory if the processing is likely to result in a high risk to individuals, or meets specified criteria.[2] The DPIA will also need regular review to reflect any changes.

15. We welcome HMRC's stated approach to carry out DPIAs for new processing activities which are likely to have the highest risk to the rights and freedoms of individuals, especially where changes to HMRC's statutory powers are proposed or where new legal gateways are created to share personal data with other public sector bodies and tax authorities. Undertaking a DPIA will likely assist in all circumstances where HMRC plans to process personal data, and will help HMRC identify potential risk, as well as helping to fulfil HMRC's requirement for accountability.

Data mapping and data sharing

16. Efficient sharing of data in the public sector can improve insights and outcomes, and increase options for recipients. Data protection law provides a framework to ensure processing of personal data is fair, lawful and transparent.

17. HMRC makes the case for collecting more data for a range of purposes connected with its functions as a tax authority, including identifying certain compliance risks and in order to reduce administrative burden on taxpayers. However, data sharing is also a key part of HMRC's proposals, which involve sharing of information with government to assist in future policy design, for example to encourage business to offer more high quality employee training and incentives, or to understand individuals sectors to allow for more targeted interventions.

18. HMRC will need to map out potential data flows as part of a data protection by design approach, clarifying specific areas of challenge and opportunity, and areas that might present risks to individuals. Any data mapping exercise will feed into the DPIA and will form part of the overall assessment it contains. It should also be kept under review and reflect any changes over time.

[2] Data protection impact assessments | ICO

19. Before sharing data, HMRC will also need to ensure that it has established a clear framework for any data sharing with government departments, devolved administrations or other organisations. Data sharing agreements set out the purpose of data sharing, including what happens to the data at each stage. They also help everyone participating in the data sharing to be clear about their roles and responsibilities. All public authorities will also need to include details of the types of information they include in their freedom of information publication schemes. The ICO's data sharing information hub,[3] which includes the ICO's data sharing code, provides valuable resources in this context.

20. If HMRC does not need personal data to achieve its objectives for itself, or when sharing with others, then it should seek to use anonymous information instead. This might be appropriate, for example, when focusing on the activity of a particular trading sector. In such cases, HMRC or government might benefit from statistical information to help design and evaluate policy interventions, but may not necessarily need data that links to individuals. In other cases, using privacy enhancing technologies (PETs) where appropriate as part of a data protection by design approach will minimise personal data use, as well as maximising security and empowering individuals.

21. We have published a call for views on our draft guidance on anonymisation[4] which is likely to be of assistance in this respect.

Necessity and proportionality

22. It will be for government to legislate to provide HMRC with the statutory powers to collect additional data where these do not already exist. However, in addition, most of the potential lawful bases for processing under UK GDPR require the processing to be necessary.[5] Necessity in this context is closely linked to the need for proportionality, and together, these principles help to establish that the processing is fair and results in fair outcomes. Controllers need to be satisfied that the processing is a targeted and proportionate way to achieve the aim and that the aim cannot be achieved in a less intrusive way.

[3] Data sharing information hub | ICO
[4] ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance | ICO
[5] Article 6 UK GDPR

23. The principles of necessity and proportionality are closely linked to the data protection principles of purpose limitation,[6] data minimisation[7] and accuracy[8]. As part of a data protection by default approach, HMRC will need to ensure, for example, that it will only process the personal data that is necessary to achieve its specific purposes and that the personal data it collects and shares is adequate for those purposes. The processing also needs to be transparent[9], and HMRC must ensure that the required technological and organisational measures are in place.[10]

24. HMRC will also need to assess necessity and proportionality in the context of potential impact on individuals. Giving consideration to such matters will assist in identifying areas of potential risk, or opportunities for pursuing more privacy-focused options, for example, by using PETs when analysing the data to reduce the risk to individuals.

25. HMRC will need to scope out how each of the data protection principles will apply for each additional area of data that it now proposes to collect, and also how they will apply to each of the circumstances in which personal data might be shared.

Transparency and fairness

26. Making clear at the outset why HMRC will collect personal data and how and why it will share it are, as mentioned above, vital elements of a data protection by design and default approach. Being clear, open and honest about the processing is also likely to promote public trust and confidence. Taking this approach will therefore help to ensure that the processing is fair and transparent. This approach also means that data protection issues can be addressed and factored into the plans for HMRC's processing at the earliest possible stage.

27. In the event of any data sharing of personal data, HMRC and the other relevant organisations will need to adopt a coordinated approach to ensure that the data processing and sharing is transparent and fair. This

[6] Principle (b): Purpose limitation | ICO
[7] Principle (c): Data minimisation | ICO
[8] Principle (d): Accuracy | ICO
[9] Principle (a): Lawfulness, fairness and transparency | ICO
[10] Principle (f): Integrity and confidentiality (security) | ICO

will include considering how they can provide meaningful privacy information to individuals in ways that will be clear and understandable.

28. In the same vein, HMRC will also need to provide clear frameworks so that the organisations involved can support individuals' rights and individuals will know how to exercise them.

29. All transparency measures will need regular review to ensure that they are fit for purpose as the policy develops.

International transfers

30. It is not clear at present whether HMRC will make any international transfers of personal data, arising by reason of the additional data that HMRC proposes to collect. HMRC should however keep this issue in mind to ensure that, if this becomes a relevant factor, it is able to undertake any restricted transfers compliantly and transparently.[11]

Consultation

30. We welcome the opportunity for engagement with HMRC on these proposals. We also look forward to receiving a formal request for consultation as required under article 36(4) UK GDPR in relation to any legislative proposals involving processing that government may look to introduce.

[11] International transfers after the UK exit from the EU Implementation Period | ICO