The Information Commissioner’s response to the Cabinet Office’s consultation on better use of data

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003, as amended (PECR). He also deals with complaints under the Re-use of Public Sector Information Regulations 2015 (RPSI) and the INSPIRE Regulations 2009.

2. The Information Commissioner’s Office (ICO) is the UK’s independent authority set up to uphold 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.

Introduction

3. The Information Commissioner welcomes the opportunity to respond to this consultation and was pleased to be involved in the open policy making process provided by the Cabinet Office and facilitated by Involve. Our response provides general comments on the overarching themes of the consultation, followed by more detailed comments on each of the specific proposals. The Commissioner’s response to specific questions is restricted to those that fall within his remit.

4. The Commissioner recognises the potential benefits of justified, sensible data sharing and how it can help improve the delivery of public services and improve policy decision making. We have always made it clear that data protection should not be a barrier to necessary and appropriate data sharing, and this is emphasised in our statutory Data Sharing Code of Practice. Large scale sharing of personal data across government and beyond inevitably engages privacy concerns and must be shown to be justified and proportionate. This is particularly the case for proposals involving bulk data sharing and the use of big data analytics. As more data is shared ever more widely and big data analytics are used in complex and unexpected ways, it

will be particularly important to consider from the outset the privacy risk, the possible impact on individuals, and how to promote transparency so that people understand how their data is going to be used.

5. There is a clear need for extensive data sharing to be accompanied by robust safeguards and the focus of our response is on whether the proposed safeguards in the consultation paper are sufficient and align with data protection obligations. The consultation paper explains that the package of legislative proposals has been designed to sit alongside rather than override existing powers or legislation which enable public authorities to access or disclose information. The new EU General Data Protection Regulation (GDPR) and Directive have both now been adopted and will come into force in 2018 following a two year transition period. The forthcoming GDPR includes stronger provisions on processing only the minimum data needed, requirements on clear privacy notices, explicit requirements for data protection by design and default, and for carrying out Data Protection Impact Assessments (DPIAs). There will have to be a thorough consideration of the impact of the new EU legal framework on any proposed data sharing legislation, including any government decisions on implementing the legislation.

General comments

6. It is important that any provisions that may increase data sharing inspire confidence in those who will be affected. Our research shows that the public are concerned about who their data is shared with and reflect concerns that they have lost control over how their information is used. Even apparently well-meaning sharing of data such as GP patient records for research purposes can arouse strong opinions.

7. We welcome the emphasis in the paper on a permissive approach to providing legal gateways to enable data sharing rather than on mandatory powers obliging public authorities to share. This positive, enabling approach to legislating for data sharing has advantages over automatic or mandatory obligations to share government data and will enable organisations to make balanced decisions in line with the DPA on whether the proposed data sharing is justified and proportionate.

8. We also support efforts to constrain the powers in the Bill by enabling specific data sharing rather than a wide, generic power to share all government data. Parliament made it clear during the passage of the Coroners and Justice Act 2009 that it did not support a very broad generic power for public authorities to share data, but we recognise that improvements can be made to legislation to enable more flexible and faster decisions enabling data sharing within government. It is
clear from our experience of working with public authorities that some practitioners continue to be confused on whether they can share data. Although the current system of establishing legal gateways for particular data sharing activity can be confusing for practitioners, we acknowledge that combining a number of legal gateways for sharing government data in one piece of legislation could help improve understanding of what the law allows.

9. The law must continue to protect individuals from excessive, unnecessary or disproportionately intrusive data sharing. We welcome, therefore, the key guiding principle behind the proposals that the powers of the DPA should not be weakened and that the proposals should be aligned with the DPA data protection principles. There is also a welcome emphasis on proportionality, and on the need for data minimisation and security. The consultation emphasises the benefits to the citizen of improved online services. A key principle of the DPA concerns individuals’ rights and we would wish to see this emphasised in any subsequent codes of practice.

10. We support the proposal to have a review of the powers in relation to the use of pilots for the fraud and debt proposals and welcome the proposal that this will be carried out in consultation with the ICO. It may be helpful to consider whether there should be wider provisions for post-legislative scrutiny in the primary legislation, especially for the more privacy intrusive proposals where civil society organisations continue to have concerns. A sunset clause or some form of periodic review of how the data sharing has worked in practice, whether it has been proportionate and whether the safeguards are working effectively could help build confidence and trust in government data sharing.

11. The illustrative clauses contain provisions for Ministers to specify in the statutory instruments the names of the public authorities to be involved in the sharing but there is not a requirement to specify the nature of the data to be shared or the purpose for doing so. This detail should be subject to effective Parliamentary scrutiny. We understand that this will provide more flexibility, but we would wish to see a requirement in the codes of practice that this information should be clearly set out in the Privacy Impact Assessments (PIAs). There is a reliance on codes of practice to provide additional details and safeguards. It is important that the likely content of these codes is available for scrutiny during the passage of any eventual data sharing legislation, so that the whole regulatory framework including any limitations is clear.
Definitions of personal data and other terminology

12. The proposed legislative proposals include a number of definitions of types of data and the organisations that will share it, which differ from the terminology used in data protection legislation. The ICO does not seek to have a monopoly on the approach taken to defining the various types of data that will be used in the data sharing process but the decision on what is and what is not personal data is a basic one and widely understood. We think there are advantages in aligning the terminology, as far as possible, with that used in the DPA and in future the GDPR; otherwise there is a risk that practitioners will be confused about whether ‘identified data’ or ‘personal information’ as used in the illustrative clauses may or may not be personal data.

Definitions of de-identified, anonymised and pseudonymised data
13. Under current data protection legislation, anonymised data – data from which no individual can be identified or is reasonably likely to be identified – is not personal data and is not subject to the DPA. The ICO’s ‘Anonymisation Code of Practice’ explains the process of converting personal data into a ‘safe’ anonymised form and stresses the importance of assessing re-identification risk in particular circumstances. Although government departments or public bodies may need a power in the legislation to share and link de-identified data, provided this data is anonymised to the standard in our code, these activities are not subject to the DPA if the de-identification process has effectively anonymised the data.

Definition of personal information
14. In the illustrative clauses provided for in some of the strands, the definition of ‘personal information’ differs from the definition of personal data provided in the DPA. The definition of personal information appears to have been taken from section 39 of the Statistics and Registration Service Act 2007 (“SRA”). This would be a wider definition than that of personal data under the DPA. Most notably, the draft clauses define ‘personal information’ to include information which relates to a body corporate. Personal data, as defined in the DPA, includes information about a living person where this person can be identified from those data and other information in the possession or likely possession of the data controller. It is also not clear in the illustrative clauses if ‘personal information’ includes information about deceased persons, which again is not covered by the DPA. While the government may want to include a wider definition of the ‘personal information’ to be shared, there is potential for confusion between ‘personal data’ and ‘personal information’. The


27.04.2016 Version 1.0
confusion that is likely to arise may be exacerbated by the provisions in the draft legislation which identify the types of personal information to be excluded from certain of the data sharing powers. This could also have an impact on safeguards because the ICO only regulates the use of personal data defined in data protection legislation.

**Definition of public authority**
15. Several of the strands include a wide definition of public authority to include a person or body entirely or substantially funded from public money. This has the potential to expand the definition of public authority to include many otherwise private or third sector organisations. The proposed scope of “public authority” under the fraud and research strand proposals in particular may need to be clarified so that we can fully understand the potential information rights implications.

**Safeguards**
16. Large-scale data sharing will require robust compensatory safeguards; these include organisations being clear about the law through ensuring there is practical guidance, including statutory codes, which help with compliance with the law and the implementation of safeguards. We support the emphasis in the consultation on the importance of safeguards, including an extension of sanctions, statutory codes of practice, the use of PIAs and the use of pilots for the fraud and debt sharing proposals. We also welcome the proposed involvement of the ICO, for example, through requirements to be consulted on codes and through undertaking audits – although of course there will be resource considerations that must be addressed to ensure that the system of supervision is sufficiently robust to inspire public confidence.

**Sanctions for unlawful disclosure**
17. The consultation includes a proposed new criminal offence of unlawful disclosures which is consistent with existing sanctions for HM Revenue and Customs (HMRC), the Department for Work and Pensions (DWP) and information held by the UK Statistics Authority (UKSA) and Office of National Statistics (ONS). There are a number of open questions about this sanction including who will enforce this offence and whether it will just apply to data controllers relying on the new powers. The role of the ICO and the interplay between the new powers and existing sanctions is also not clear. It will be important to work with the ICO and others to ensure enforcement powers are sensible and do not create further confusion or conflict.
18. There are a number of enforcement tools available to the ICO for taking action against organisations who breach the DPA. They include criminal prosecution, non-criminal enforcement and consensual audits. The Information Commissioner also has the power to serve a monetary penalty notice imposing a financial penalty of up to £500,000 for serious breaches of the DPA. If an organisation or an individual successfully re-identify data, then in DPA terms they would become the data controller for that data. If they processed personal data without making relevant parties aware and there is a risk of harm to the individuals, then the Commissioner may take regulatory action, including the imposition of a civil monetary penalty up to the maximum allowable amount. However, a potential enforcement notice or civil monetary penalty may not be an effective tool in these cases. There is merit in considering whether there should be a specific criminal offence in cases of deliberate re-identification of anonymised data.

19. On some occasions it is not the data controller that is responsible for data protection breaches; it is an individual acting in contravention of an organisation’s policies and procedures, or an individual who obtains information from an organisation without their knowledge or consent. Section 55 of the DPA makes it a criminal offence to knowingly or recklessly – and without the consent of the data controller – obtain, disclose, or procure the disclosure of personal data. This offence is currently punishable by fine only. Section 77 of the Criminal Justice and Immigration Act 2008 includes a provision for introducing custodial sentences for the DPA section 55 offence; this has not yet been commenced. The Information Commissioner continues to call for more effective deterrent sentences, including the threat of prison in the most serious cases, to be available to the courts to stop the unlawful use of personal data. Strengthening this sanction would make it more consistent with the proposed new criminal offence of non-disclosure.

**ICO audits**

20. There are references to the ICO undertaking audits of public authorities’ data sharing. We would welcome discussions on these proposals; for example, whether we would need to have powers to follow the shared data across organisations and mandatory audit (assessment notice) powers to do this in certain sectors. A number of sectors such as local authorities are currently outside the scope of compulsory audit so there would need to be consideration of the scope of the audits and whether the assessment notice power would be extended to them. The ICO’s powers of compulsory audit could provide more effective regulation of data sharing in these sectors but
If the audits were to be compulsory there would be resource implications for the ICO.

Codes of Practice

21. We support the use of codes of practice as a flexible instrument. Given the reliance on codes of practice to provide additional details and safeguards, it is important that the likely content of these codes is available for scrutiny during the passage of any future data sharing legislation so that the whole regulatory framework, including any limitations, is clear. It is also critical that these codes be kept up-to-date, and we suggest that a requirement be included in the provisions of the legislation to regularly update the codes.

22. The draft illustrative clauses leave the detail of the proposals fairly open, presumably relying on the codes of practice to define procedures and fill any gaps. The illustrative clauses require organisations to have regard to the relevant code of practice in sharing data. It is not always clear whether these codes will be statutory codes. Even if they are, it is not clear whether the failure to follow procedures outlined in the codes will be an enforceable offence. Important safeguards should be included in the legislation or, if this is not possible, they should be in codes of practice which are available for scrutiny during the passage of the legislation. We welcome the requirement for the Minister to consult the Information Commissioner in preparing these codes, which is included in the illustrative clauses; but in the absence of draft codes, it is difficult to appreciate how these codes will align with our own statutory Data Sharing Code of Practice.

23. In the ICO’s experience, where organisations have been required to work with multiple codes of practice in their sectors, and the advice in these codes conflicts this has caused confusion and uncertainty. It will be important to ensure that any new code minimises confusion and the risk of providing conflicting advice. Organisations using these proposed data sharing powers may also find that other legislation to which they are subject conflicts with the permissive powers and/or codes of practice. It is not clear from this consultation document how such conflicts will be resolved.

Privacy Impact Assessments (PIAs)

24. We note that organisations will be required to prepare PIAs in line with our code of practice and publish them for public scrutiny. We welcome this safeguard, and note that it could help data controllers prepare for new requirements for DPIAs under the GDPR. There is no statutory requirement to produce PIAs at present; how such a duty would be
enforced requires thought. Although including the requirement within any new legislation is preferable, it may be possible to have a requirement in a statutory code of practice. To ensure this happens, any legal provisions requiring a code could make it clear that its provisions must include requirements on the undertaking and publication of PIAs.

25. The GDPR will require DPIAs for certain activities and prior approval from the national supervisory body, which is likely to be the ICO in the UK. The ICO will also be required to produce a list of processing activities for which data controllers will be required to prepare a DPIA. Beyond these future requirements, however, is not clear who, if anyone, will be responsible for reviewing the PIAs or what will happen if the assessment reveals a substantial privacy risk that cannot be sufficiently mitigated. If there is to be oversight, then resourcing of the eventual supervisory body may be an issue for consideration.

Transparency

26. We welcome the focus on transparency in various parts of the consultation paper, such as the recommendation that PIAs should be published proactively. Transparency and accountability are important elements of building trust and confidence in the government’s use of data but transparency and clarity for individuals is also very important. Combining different information from different sources can create a very detailed picture of an individual’s affairs and thought will have to be given to how government is going to explain this and its likely consequences. The ICO has consulted on a revised Privacy Notices Code of Practice\(^3\) in order to provide more guidance on how to make privacy notices more engaging and effective, and to emphasise the importance of providing individuals greater choice and control over what is done with their data where that is appropriate. The ICO has developed this code with compliance with the GDPR in mind, as well as where the law stands today. The GDPR will require enhanced transparency and accountability by organisations.

Big data and analytics

27. Big data increases the risk that individuals may be re-identified from apparently anonymised datasets. If an organisation or an individual does this, then in DPA terms they become the data controller for that data. They take on all the responsibilities of a data controller, including telling the individuals concerned that they are processing

their personal data. If they process personal data without their knowledge, and there is a risk of harm to the individuals, then the Commissioner may take regulatory action, including the imposition of a civil monetary penalty of up to £500,000. We propose that there is merit in considering whether the introduction of a specific criminal offence would be more appropriate and provide a stronger deterrent for those who deliberately seek to re-identify individuals. The ICO has also welcomed the work of the Cabinet Office on data science and ethics, in particular the ethical framework.

**Health and social care data**

28. We note that the current proposals exclude the use of health and social care data, in part due to the impending publication of Dame Fiona Caldicott’s consent review. The DPA does not prevent sharing health and social care data, provided this is consistent with the data protection principles, including a legal basis and relevant Schedule 2 and 3 conditions for doing so. The inclusion of health and social care data may be essential to success in certain strands, particularly Improving Public Services. Principle 3 of the DPA in particular is worth considering, and whether excluding certain categories of data would jeopardise the adequacy of processing, eg for improving public service delivery and research. As sensitive personal data, it will be important to include appropriate safeguards, but in principle there is no data protection barrier to including health and social care data. The GDPR includes provisions concerning processing of health data specifically – and special (ie sensitive) personal data more generally – that should be considered if health and social care data is included.

**Comments on detailed proposals**

**A – Improving public services**

i) Improving public service delivery

**General Comments**

29. The proposal provides a permissive power for sharing data for more targeted public service delivery. The power will relate to specified public authorities. In our experience, public authorities involved in this delivery often already have a legal gateway for sharing information and the power to share does not have to be expressly provided in law. Consequently, many initiatives to improve public service delivery, such as Troubled Families, are able to proceed under the current legal framework. This power will be helpful insofar as it provides certainty
of the legal gateway; however, it may not resolve several key challenges, such as reluctance to share with private and third sector organisations. It also does not resolve the issue of finding appropriate conditions for processing under the DPA, which has been a challenge for some programmes.

30. Programmes such as Troubled Families often involve multiple purposes over several stages and not just the intervention itself. This includes data processing to narrow down those individuals in need of the intervention, and evaluation of the programme, which are different purposes and often present different privacy risks. If the proposals are intended to cover the full scope of such programmes, then it will be important to ensure this is clear in the legislation and that each stage is addressed in the required PIAs and the Code of Practice for this strand.

**Specific questions**

**Q1. Are there any objectives that you believe should be included in this power that would not meet these criteria?**

31. In the consultation paper, one of the two objectives is “improving the ability to identify families who would benefit from the Troubled Families programme”. This implies a fairly narrow scope, but the illustrative clauses seem broader, ie “identifying individuals or households who face multiple disadvantages and enabling public services to be provided to such individuals and households to be tailored to their needs”. Further clarification, possibly through the open policy making process, would be helpful.

**Q2. Are there any public authorities that you consider would not fit under this definition?**

32. If health and social care data is included, this list of public authorities will need to be expanded to include relevant health bodies.

**Q3. Should non-public authorities (such as private companies and charities) that fulfil a public service function to a public authority be included in the scope of the delivering public services power?**

33. To avoid confusion, the definition of ‘public authority’ should not be expanded to include private and third sector organisations, but there could be value in expanding the scope of the power to include such organisations, when it is necessary to achieving a particular purpose. The absence of a legal gateway for third sector organisations is often cited as a barrier in data sharing initiatives. Some public authorities do not feel comfortable sharing with organisations without a legal gateway. Whilst a statutory gateway provides legal certainty when a
public authority shares personal data, the data protection principles would allow the sharing anyway, provided it is done in compliance with the data protection principles - and provided that the sharing is necessary for the public authority’s or government department’s statutory or common law purposes and is not therefore ultra vires. Given the growing importance of private and third sector organisations in delivering certain public services and the reluctance of public authorities to share without an explicit gateway, it is a matter for the government to decide whether expanding the scope of this power would be an appropriate measure. As noted in the consultation paper, this could also provide consistency in the conditions and safeguards across public service delivery.

Q4. Are these the correct principles that should be set out in the Code of Practice for this power?

34. The principles refer to ‘additional safeguards’ in addition to those existing in legislation such as the DPA. It is not, therefore, clear whether the DPA will be covered in the Code of Practice. Given that our Data Sharing Code of Practice is general in nature, it would be helpful for the code to provide good practice measures to comply with the DPA, focused on the delivery of tailored public services.

ii) Providing assistance to citizens living in fuel poverty

General Comments

35. We recognise that this measure is about efficient targeting of public services to those with most need. Data protection should not be a barrier to necessary and appropriate data sharing to assist those who are living in fuel poverty. The primary barrier at present appears to be the lack of a legal gateway to share individuals’ data to allow matching across data sets to occur, which this measure addresses.

36. We welcome this proposal as an example of a ‘constrained power’ for limited purposes. This approach should assist in gaining public support, as it provides some reassurance that data permitted to be matched for this specific purpose will not be used to disadvantage individuals.

37. The number of individuals that could be affected by this proposal is also unclear because the definitions are left quite open. The definition of fuel poverty in the draft clauses (at section 1(3)) does not specify what a ‘lower income’ and ‘reasonable cost’ is. Low incomes and higher-than-typical heating costs are blamed for the most severe
cases of fuel poverty. It therefore appears that millions of individuals are likely to be affected by fuel poverty, but the proposal to share these individuals’ data has not been subject to the same level of scrutiny as other strands because it was not part of the open policy making process.

Specific questions

Q5. Should the Government share information with non-public sector organisations as proposed for the sole purpose of providing assistance to citizens living in fuel poverty?

38. We support the approach of minimising the extent of data sharing outside the scheduled public sector organisations as a safeguarding measure. The consultation paper states that non-public sector organisations will be provided with an eligibility flag and the eligible individual’s name and ‘equivalent unique identifiers’. We are interested in what these unique identifiers will be and suggest this could be part of the open policymaking process. We would also support the proposed safeguard to limit the purpose for which this information is being used, but note that the proposal also suggests a further purpose, ie promoting energy efficiency measures.

39. The objectives in the draft clauses also suggest a broader remit than in the consultation paper. The objective at 1(2)(b) is: ‘reducing the energy costs of, or improving the health or well-being of, people living in fuel poverty’. This may suggest that the manner in which assistance is provided to individuals extends beyond the automatic discount applied to energy bills as outlined in the consultation document. The definition of well-being is left very open, which could lead to wider application of the powers than originally intended. This is an issue that the government might want to consider further.

Q6. Would the provision of energy bill rebates, alongside information about energy efficiency support, be appropriate forms of assistance to citizens living in fuel poverty?

40. From an information rights perspective, the two purposes are separate proposals with different considerations. Providing energy bill rebates automatically through data sharing within the government has a clear benefit for individuals, and it makes sense to share that information to determine eligibility. Even though the assistance is automatic, it will still be important to tell individuals how their data is being used and who it is being shared with in order to comply with the requirements of the DPA, including the first principle.
41. Although providing information about energy efficiency could also benefit the targeted individuals, it is not clear in the consultation paper how this information will be conveyed and whether it will engage PECR. It may not be within individuals’ expectations to receive this information from their energy providers, which are private companies. If the provision of information constitutes direct marketing under PECR, it is not clear from this consultation how consent will be obtained. Under the forthcoming GDPR, the establishment of clear consent will be even more important.

Q7. Are there other forms of fuel poverty assistance for citizens that should be considered for inclusion in the proposed power?

42. It is not for the ICO to determine what other forms of assistance should be considered. However, where other forms of assistance are considered, it will be essential to consider whether new purposes are being introduced and how personal data is used to achieve these additional purposes. Beyond the legal gateway, any additional forms of assistance will still require relevant conditions for processing personal data, including for sensitive personal data (where applicable). The measures will also need to be fair and consistent with the expectations of the individuals concerned, and organisations providing assistance will need to ensure that individuals are aware of how their data is being used and shared for the provision of these additional assistance measures.

iii) Increasing access to civil registration information to improve public service delivery

General Comments

43. This proposal was added at a relatively late stage of the open policy making process and has not been subjected to the same degree of scrutiny as other measures. As is the case with the other measures, the emphasis in the legislative clauses is on which organisations will be sharing the data, rather than what data will be shared and for what purposes. The sharing of data for more convenient and secure citizen access to government services is likely to enjoy more support than vague proposals for bulk sharing of data to assist public authorities to fulfil their functions. There is also justification for sharing information to track down forged or altered certificates. Civil registration information can be very sensitive, including information on adoptions and still births. We welcome the requirement for a statutory code of practice, to be prepared in consultation with the ICO. Given this is a discretionary power for the Registrar General, it may be helpful to establish a Strategic Steering Group (SSG) along the lines of that
proposed for combating fraud to help decide whether data sharing proposals are justified and proportionate.

Specific questions

Q8. Should a government department be able to access birth details electronically for the purpose of providing a public service, e.g. an application for child benefit?

44. The government’s plan to reduce the circulation of official identity documents, and reduce the potential for fraud, is welcome; and the purpose of providing public services through more convenient and secure mechanisms is likely to have broad public support. For example, we are aware that the sharing of data between the Passport Office and DVLA, allowing drivers’ identities to be verified without the inconvenience of sending sensitive documents through the post has proved to be popular with drivers. The wording of the current proposals, in enabling ‘access’ for these purposes does not provide clarity on the method of transfer as proposals refer to ‘verification or sharing’ of data.

45. The verification of birth and death records using Application Programming Interfaces (APIs) – accessing a central record in order to confirm that the event took place – would minimise the amount disclosed and fit better with DPA. If access did involve sharing, any statutory code of practice would need to investigate thoroughly the potential for any disclosure to infringe upon a data subject’s article 8 rights to privacy.

46. Current statutory safeguards apply around the disclosure of birth records for adopted individuals. There are similar safeguards around gender recognition records; but only where an individual has lived with their acquired gender for at least 2 years, and applied to the Gender Recognition Panel for a new certificate; for applications by the standard route. Where the purpose is confirming if an event took place, marriage records may not be as reliable a source as birth and death records. As divorce records are held by Her Majesty’s Court & Tribunal Service (HMCTS), not the General Registrar’s Office (GRO), additional linking would be required in order to provide assurance on the accuracy of the data, depending on the purpose required.

47. Any sharing of marriage or civil partnership data could require an additional condition for processing as this data by its nature discloses sexual orientation. In most cases this is also likely to disclose data related to two data subjects, both of whom would require fair processing.
48. Any code and PIA process would need to cover the issues above, specifically in the context of the first data protection principle where it applies and whether data was processed fairly. Improving public services may not always align with the wishes or expectations of individuals, specifically in the context of bulk sharing with no meaningful opportunity to provide or withdraw consent.

Q9. Do you think bulk registration information, such as details of all deaths, should be shared between civil registration officials and specified public authorities to ensure records are kept up to date (e.g. to prevent correspondence being sent to families of a deceased person)?

49. The Tell Us Once service has always been a voluntary service based on the families providing consent. We are not clear whether the proposed service will replace this service.

50. It is worth noting that the DPA cannot be relied upon as a safeguard for death records, where they do not link to third parties who are natural living persons, as this information does not meet the definition of ‘personal data’ in the DPA. A power to share death records in bulk for the purpose of list cleaning could work similarly to the current Disclosure of Death Registration Information (DDRI) scheme provided by GRO. DDRI has narrow gateways permitting sharing for the specific purposes of ‘to prevent, detect, investigate or prosecute offences’.

51. As currently drafted, bulk sharing for ‘relevant private companies’ (as referred to in the attached Impact Assessment) for purposes such as fraud prevention would provide broader access than currently possible the DDRI with fewer safeguards. DDRI can disclose to specific types of organisations (rather than relevant organisations) with additions to the list possible by order. DDRI also allows GRO to add requirements to a disclosure as a condition on primary legislation (s13(4) Police & Justice Act2006). These requirements can relate to restricting the onward disclosure of bulk data from license holders, and specifying retention schedules. Finally, GRO can require quarterly data from licence holders to evidence their use of data under their license agreement remains consistent with the specified purpose of disclosure. It should be noted that the level of safeguards deemed adequate for a death record may not be adequate for records of other life events.

52. The consultation document references a mandatory requirement for ‘deletion of bulk data once data has been used for that purpose’. Further consideration of definitions for this safeguard may be required in the Code of Practice, as data could be legitimately held by authorities for the same purpose or function for varying lengths of time. Although this question refers to death records specifically, the
illustrative clauses as drafted could allow for the sharing of other life event records. Some proposed applications will use bulk data to identify patterns which may suggest fraud, searching for a causal link between the individual and the commission of offences. This could have implications for data controllers, who would be unlikely to satisfy a s29 or s35(2) exemption from subject access, and again raises concerns around accuracy and fairness for data subjects, many of whom would not be under investigation themselves. Such processing of personal data could engage issues of privacy and article 8 ECHR rights, as well as the ability for data subjects to assert their rights under the DPA, or the forthcoming GDPR (eg the right to subject access and the right to object to automatic processing).

B – Tackling fraud and debt

i) Combating fraud against the public sector

General Comments
53. As the paper acknowledges, there are numerous existing legislative gateways that enable public authorities to share data for the purposes of combating fraud. We have observed that frequently these provisions are under-used or ignored. During the open policy making process, civil society groups felt that further evidence was needed on data sharing in this sector. We support the use of pilots and the emphasis on post-legislative scrutiny where the relevant Minister would assess the success of the projects and determine whether it should proceed or be terminated. We were not clear whether there would have to be further legislation enabling the pilots to become permanent data sharing arrangements. Any evaluation of the pilots should consider privacy and data protection compliance, and we recommend that a further PIA should be undertaken at that point.

54. We welcome the proposed safeguards in the consultation document, in particular the requirement for a statutory code and the proposal that the legislation states explicitly that data cannot be disclosed under the new power if it contravenes the DPA or Part 1 of the Regulation of Investigatory Powers Act 2000. It is also proposed that organisations will have to make a business case for any data access arrangement. Information in the business case will include methodology, costs and benefits etc. It would be helpful if organisations also considered the privacy impact at this point and were assisted in considering privacy risks and the justification for their proposal in detail. The creation of the SSG within this measure is also a positive step and would help improve oversight over what could be extensive and privacy-intrusive data sharing. We see that it is proposed to include representatives from civil society organisations and other independent observers, and
the ICO would be happy to participate in that capacity if it was considered useful.

Specific questions

Q10. Are there other measures which could be set out in the Code of Practice covering the proposed new power to combat fraud to strengthen the safeguards around access to data by specified public authorities?

55. We consider that the code of practice should require regular reviews of the pilots, particularly given the likely development of big data and use of analytics. There will also be a need to ensure prompt resolution of false positives and rectification of data so they do not recur. It may be necessary to end pilot schemes early if they result in high false positive rates, especially where inaccurate information results in serious consequences for individuals, particularly if they have done nothing wrong.

56. A clause requiring the code of practice to be reviewed regularly on a set timescale would enable novel datasets or new data matching techniques to be used in a timely manner without requiring government to act in contravention of a statutory code. There are current codes of practice governing data matching that have not been updated for some time, and a statutory requirement to review and reissue the code would guard against this and provide an additional safeguard, perhaps including parliamentary scrutiny.

57. Use of APIs would require greater consideration of information security under the DPA and a code of practice could usefully remind people of this. A short, blanket retention period for data that is shared could be considered under the code of practice to ensure that published information is disposed of by the public authority with which it is shared on an appropriate timescale.

58. The code of practice would appear to be applicable to the data of bodies corporate. This data could be shared without contravention of the DPA as it is not personal data under that Act or under the proposed GDPR. If ICO audits are to be a safeguard, they could either be of a sample of organisations; or all organisations involved could be audited. This could have resource implications for the ICO and a timescale would be useful in the code of practice to indicate the frequency of audits.
Q11. It is proposed that the power to improve access to information by public authorities to combat fraud will be reviewed by the Minister after a defined period of time. This time will allow for pilots to be established and outcomes and benefits evaluated. How long should the fraud gateway be operational for before it is reviewed?

59. Consideration would need to be given to how long data could be regarded as suitable for the purposes being pursued. Retention schedules for different types of data can drive changes in how data is recorded and therefore its relevance to the task. Further research into the life cycle of government data, and the period for which it remains a useful and usable data resource, would need to be considered in setting a time limit.

ii) Improving access to data to enable better management of debt owed to the public sector

General Comments

60. The illustrative clauses governing the debt measures are very similar to the clauses governing the fraud measures. However, among other differences, under the DPA the condition for processing data for fraud combating purposes is different to the condition for processing data for the purposes of managing public sector debt. The code of practice would have to treat fraud and debt as separate measures because of this.

Specific questions

Q12. Which organisations should Government work with to ensure fairness is paramount when making decisions about affordability for vulnerable debtors who owe multiple debts?

61. Again the proposal for a business case to be produced should encourage full consideration of the proposals; but we also want to see privacy considerations built in at this stage, in particular whether proposals are justified and proportionate – not just whether they would reduce debt. Any proposed data sharing would have to be backed up by clear purposes for sharing between government departments, for example to gain a single debtor view and therefore help debtors. Again a pilot programme for this measure may be helpful, and any evaluation of the pilot should include privacy and data protection issues. We are also not clear whether the data sharing can
go ahead after the pilot or whether there would need to be further legislation for it to continue. The consultation paper does not mention any governance of the debt strand other than a review of the power; something similar to the SSG proposed for fraud might be useful here.

**C – Allowing use of data for research and for official statistics**

i) Access to data which must be linked and de-identified using defined processes for research purposes

*General Comments*

62. This proposal introduces a number of safeguards to ensure processing of personal data for research purposes is done in a secure, justified and proportionate way. The draft illustrative clauses state that data cannot be supplied if it contravenes the DPA. De-identified data is a term widely used and understood within the statistical and research communities, but some practitioners working outside those fields may not be clear whether some of the information mentioned in the proposals and illustrative clauses is personal data for the purposes of the DPA.

63. Some pseudonymised data can be anonymous, the most obvious case being where the personal data from which the pseudonymised data was generated has been deleted and where there is no other ‘matchable’ data that might allow re-identification to take place. There is a spectrum of personal identifiability based on the nature of the information itself and on other factors, such as the availability of matchable information. We accept that this can sometimes make it difficult to draw a clear distinction between personal data and non-personal data. As described in the proposal, it appears that some ‘de-identified data’ may be pseudonymised data. If the intention is that this be non-personal data for the purposes of the DPA, then understanding the legal concepts and applying the tests outlined in our Anonymisation Code of Practice would help ensure that standard is met. Whether the data is personal data or anonymised (and thus no longer personal data) may need to be evaluated on a case-by-case basis.

64. We would also note that the objective of the proposal is to enable research for public benefit, but such research often requires the processing of personal data. Such processing can be done in a way that complies with the DPA. In our experience, many public authorities are reluctant to share personal data for research purposes, even when such sharing could be done lawfully under the DPA. This reluctance can be due to a lack of understanding about data protection law, or arise from concerns about compliance with other laws, such as the
common law duty of confidence. This contributes to uncertainty about when personal data can be shared, so the proposals could provide more clarity for organisations regarding what data they can share, and when they can share information that is fully anonymised versus pseudonymised or de-identified.

65. Under the proposal, accreditation is recommended for indexers, researchers, access facilities and the research itself, with the UKSA as the proposed accreditation body. It will be important at the outset to establish which organisations are data controllers and which are data processors in these relationships in order to clarify the data protection responsibilities of the bodies involved. Given this extensive remit, there are a number of practical matters regarding this accreditation that will need to be addressed. For example, at present, the draft illustrative clauses do not include a mechanism to monitor/audit these facilities once they are accredited. This is a key issue to consider once facilities are accredited and could require significant resources.

66. There are further safeguards that could be considered, for example, if the accredited facility does not meet the standards required then it should be possible to remove the accreditation so that the relevant organisation cannot carry out work until it is successfully re-accredited, or other appropriate sanctions applied (eg withdrawal of funding). Within the accredited facilities there should be oversight of the de-identification process, perhaps at Senior Information Risk Officer (SIRO) level.

67. Where data sharing is being done for the public good there should be a high degree of public openness. We would thus support measures to ensure transparency in this area, eg publishing a register of the datasets flowing in and out of accredited facilities.

68. The proposals include sanctions for unlawful disclosures and restrictions on further disclosure. Clarity is needed on whether these sanctions will affect current data sharing agreements that enable such disclosures, consistent with current law. We would also note that the legislation will need to be future-proofed, or reviewed under a sunset clause, to respond to the forthcoming changes under the GDPR, which has several provisions directly relevant to research and statistics.

69. With the rapid rise of big data, data science, open data and data sharing, there is a valid case that there is an increased risk that individuals may be re-identified from apparently anonymised datasets, or more likely a combination of personal data and de-identified data. The incentives to deliberately and negatively attack anonymised data are likely to become stronger as data becomes an increasingly valuable commodity, so we recommend that the government should
consider whether stronger deterrents and governance safeguards are necessary. It is also worth noting that re-identification risk can be mitigated by ensuring only the data necessary for a particular purpose is released (ie data minimisation).

70. If an organisation or an individual successfully re-identifies data, then in DPA terms they would become the data controller for that data. They would take on all the responsibilities of a data controller, including telling the individuals concerned that they are processing their personal data. If they processed personal data without their knowledge, and there is a risk of harm to the individuals, then the Commissioner may take regulatory action, including the imposition of a civil monetary penalty of up to £500,000. However, a potential enforcement notice or civil monetary penalty may not be an effective tool in these cases. We would actively support the introduction of a re-identification criminal offence which would provide a stronger deterrent for those who deliberately seek to re-identify individuals. This was an issue we raised in the recent Science and Technology Select Committee Inquiry into big data and the Committee supported the case for a re-identification offence in their recommendations4.

Specific questions

Q15. Should fees be charged by public authorities for providing data for research purposes, and if so should there be a maximum fee permitted which is monitored by the UK Statistics Authority?

71. If the government decides to introduce charges, then this could be done on the basis of reasonable recovery of costs.

Q16. To ensure a consistent approach towards departments accepting or declining requests for disclosing information for research projects, should the UK Statistics Authority as the accreditation body publish details of rejected applications and the reasons for their rejection?

72. As a matter of transparency, it would be good practice to publish such details where this complies with data protection requirements. We have supported the reasons for rejection and the name of the organisation being made public but would not go so far as to name individual researchers. In addition, the criteria that will be used when considering requests should also be published so there is a shared understanding of what aspects will be considered. Publishing a register


27.04.2016 Version 1.0
detailing the datasets flowing in and out of the accreditation body would also further the goals of consistency and transparency.

**Q17. What principles or criteria do you think should be used to identify research that has the potential for public benefit, or research that will not be in the public benefit?**

73. While specification of the exact principles is not within our remit, we note that there are several provisions in the GDPR relevant to processing data for public benefit. The full effect of the GDPR is not yet known, but any new data sharing legislation should be robust enough to accommodate future changes. The GDPR specifies that where processing is necessary for the performance of a task carried out in the public interest, the processing should have a basis in Union or UK law. The Regulation does not, however, define what is meant by the public interest so it will be helpful to outline what this means for the purposes of these proposals.

74. Under the GDPR, the UK will be allowed to introduce national provisions to further specify when the public interest provision applies. There would be advantages in having a national provision here, in terms of legal certainty and the introduction of statutory safeguards. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, UK law may also determine and specify the tasks and purposes for which the further processing shall be regarded as compatible and lawful, which could include the prohibitions on further disclosures proposed here. However, it is also notable that, in cases where the data is being processed for purposes other than the one for which it was collected, this processing could be considered lawful if it is for scientific and historical research purposes or statistical purposes.

ii) Access by UK Statistics Authority to identified data for the purpose of producing official statistics and research

**General Comments**

75. Current barriers to data sharing discussed in the document are related to current legislative barriers outside the DPA. Moving to a more flexible system to accommodate data sharing is not inconsistent, in principle, with the DPA, provided appropriate safeguards are in place. An important safeguard is provided in the illustrative clauses, wherein public authorities need not comply with an order to disclose information if that would contravene the DPA. The proposed amendment to the SRSA to give public authorities the power to disclose information to the UKSA when required to exercise its...
functions likely means public authorities could find a relevant condition for processing under the DPA.

76. This measure discusses the integrity, quality, and supply of information, and where this is personal data, there is also an interaction with the DPA that is worth noting. Principle 5 of the DPA requires that personal data should not be retained for longer than necessary, which may limit the usefulness of this measure, unless the data is processed only for research purposes, in which case it can be kept indefinitely (s33(3)). Principle 4 requires that personal data is accurate and, where necessary, kept up to date. This requirement is separate from, but complements, the emphasis on providing accurate information and the proposed criminal penalties for providing misleading information.

77. We would also note that the legislation will need to be future-proofed to respond to the forthcoming changes under the GDPR, which has several provisions directly relevant to research and statistics.

Specific Questions

Q18. Is two years a reasonable maximum period of time for the duration of a notice for the supply of data to the UK Statistics Authority for the purposes of producing National and official statistics and statistical research?

78. This question is outside our remit.

Q19. If your business has provided a survey return to the ONS in the past we would welcome your views on:

(a) the administration burden experienced and the costs incurred in completing the survey, and

(b) ways in which the UK Statistics Authority should seek to use the new powers to further reduce the administrative burdens on businesses who provide data to the ONS for the purposes of producing National and other official statistics.

N/A
Q20. What principles and factors should be considered in preparing the Code of Practice on matters to be considered before making changes to processes that collect, store, organise or retrieve data?

79. The recommendation to consult with the Information Commissioner is important, as there may be further interactions between the proposals in this strand and the DPA that need to be clarified. For example, public authorities may be required to consult with the UKSA when making changes to processes for collecting, organising, storing or retrieving information. It will be important to consider compliance with the DPA principles explicitly in such a consultation. The process for doing so, and the relationship between the UKSA and the ICO in this process, could be clarified in the Code of Practice.

Information Commissioner
April 2016